NATIONAL CYBER CRIME REFERENCE **HANDBOOK**

⏩ A Mandatory Disclosure

A Joint Initiative by

NATIONAL CYBER SAFETY AND SECURITY STANDARDS
(Editorial Board)

MINISTRY OF COMMERCE AND INDUSTRY
MINISTRY OF SOCIAL JUSTICE AND EMPOWERMENT
MINISTRY OF MICRO, SMALL AND MEDIUM ENTERPRISES
(Government of India)
(Institutional Partner)

AICTE – ALL INDIA COUNCIL FOR TECHNICAL EDUCATION
(Institutional Partner)

Published by the **Additional Director - General**
Publication Division
National Cyber Safety and Security Standards
(An Autonomous Body undertaken by NCSL)
CYBER HOUSE – Southern Region
No: 1, 1st Floor, 1st Avenue,
8th Cross Street, Indira Nagar Main Road,
Adyar, Chennai – 600 020.
Phone : 044 – 2440 1766/044-2445 1766
Fax : 0 84688 65111

Email : support@nationalcybersafety.com
Web : www.ncdrc.res.in

Publisher's Note : Inspite of our best efforts can creep in. Any mistake, misprints, missing pages or discrepancy etc., noticed may kindly be brought to our knowledge, so that it may be corrected in the next Edition. This book is a combined version of materials from various sources. So, the National Cyber Safety and Security Standards will not give any authenticity to the content.

Printed at
Sri Raj Cine Printers
Chintadripet , Chennai

The Greatness of INDIA

India “Truth Alone Triumphs”(Satyameva Jayate)

Present Scrutiny

- 5,000 Years Old Ancient Civilization.
- 530 Languages Spoken.
- 652 Dialects.
- 18 Official Languages.
- 28 States, 7 Union Territories.
- 3.28 Million Sq. Kilometres - Area.
- 7,516 Kilometres - Coastline.
- 1.23 Billion Population.
- 5600 Dailies, 15000 Weeklies and 20000 Periodicals in 21 Languages with a Combined Circulation of 142 Million.
- GDP $1840 Billion. (GDP Rate 5.5%).
- Parliamentary Form of Government World’s Largest Democracy.
- World’s 4th Largest Economy.
- World-Class Recognition in IT, Bio-Technology and Space.
- Largest English Speaking Nation in the World.
- 3rd Largest Standing Army Force, Over 1.5 Million Strong.
- 2nd Largest Pool of Scientists and Engineers in the World.

Dedicated to

Our Nation

NATIONAL CYBER DEFENCE RESEARCH CENTRE
एन सी डी आर सी

न्यायाधीश **डॉ. एस. मोहन**

Justice **Dr. S. Mohan**

Former Judge, Supreme Court of India
Chairman - National Cyber Safety and Security Standards

Foreword

I am glad to note that our National Cyber Safety and Security Standards team is publishing a book on Cyber Security domain. This book is very useful to all the people who are working in the Government Sectors, Private Sectors, Corporate Companies and especially for Educational Institutions.

Today the Cyber World has come to occupy an important place in the history of mankind. As science advances, the knowledge also expands. It is undeniable fact that Cyber World has thrown a new vista but regretfully it has to be noted that it has also being misused and spreading undesirable information. It has become necessary to find out ways and means to curb this menace of spreading evil knowledge.

We live in the electronic age in which every institution of Government, Business and Industry, big and small, and even the family interact and communicate with one another electronically. Electronic devices which process data are no longer confined to what we traditionally consider as computers, but are pervasive in everyday life. They range from mobile 'smart' telephones to global positioning by satellite devices, and from health-monitoring devices to defibrillators.

Information Security is an art, not a science and the mastery of information security requires a multi-disciplinary knowledge of huge quantity of information, experience, and skill. There is a great satisfaction knowing that your employer's information, communications, systems, and people are secure. Comprehensiveness is an important part of the game you play for real stakes because the enemy will likely seek the easiest way to attacks the vulnerabilities and assets that you haven't fully protected yet.

The past decade has witnessed tremendous legal reform by countries around the world. The most influential-electronic commerce has led countries to revise and update their rules of evidence on the proof and admissibility of such evidence. And litigants have responded by informing that courts are witnessing a myriad and a rising volume of electronic evidence tendered by the parties. These ranges from emails to mobile messages, from chat records to blog entries and even "tweets" to mobile messages, resolving the many difficult issues regarding discovery and inspection of electronic documents (or electronically stores information) and the authentication and admission of electronic evidence now calls for a technologically savvy bar.

The book entitled, National Cyber Crime Reference Handbook comprising of chapters such as Cyber Hacking, Indian and International perspective on key topics including E-commerce, Email Security, Cloud Computing, Cyber Fraud, Cyber Pornography, Cyber Crime and Cyber Attacks, Evidentiary value of a Video Conferencing, Internet, Mobile Phones, Privacy and Electronic Surveillance, Digital footprints — Assessing Computer Evidence, Monitoring, De-Cryption and Interception.

I convey my best wishes to the National Cyber Safety and Security Standards publishing committee.

(Dr. S. Mohan)

Preface

Today, the internet has turned 40, and with its maturing, the threats are increasing. Botnets and cyber-criminals are making news regularly. It has become increasingly obvious to everybody that something needs to be done to secure not only our Nation's critical infrastructure but also the businesses we deal with on a daily basis. The question is, "where do we begin?" what can the average information technology professional do to secure the systems that he or she is hired to maintain? One immediate answer is education and training. If we want to secure our computer systems and networks, we need to know how to do this and what security entails.

As global networks expand the interconnection of the world's information systems, the smooth operation of communication and computing solutions becomes vital. However, recurring events such as virus and worm attacks and the success of criminal attackers illustrate the weaknesses in current information technologies and the need to provide heightened security for these systems.

You cannot perform your job or organize your social life effectively without using e-mail and the World Wide Web. Our reliance on these technologies and the extent to which we take them for granted are a testament of the impact of the Internet and the Web on our lives. These technologies have created a better-informed consumer and a manager who is equipped with up-to-the-second information. Communities have sprung up and supply chains have been redesigned. In general, the opportunities that have been created due to the unique properties of these technologies allow us to set higher goals for our businesses and meet them more effectively.

We have now entered the world of low impact, multiple victim crimes in which bank robbers, for example, no longer have to meticulously plan the theft of millions of dollars. New technological capabilities at their disposal now mean that one person can effectively commit millions of robberies of one dollar each. Against this background, David Wall scrutinizes the regulatory challenges that Cyber Crime poses for the criminal (and civil) justice processes, at both the national and the international levels.

The National Cyber Crime Reference Handbook will comprise the detailed perspective of the Cyber Crimes which are creating massive trouble for India's National Security and also this book provides advanced cyber protection methodologies and controlling procedures/tools.

Chapter 1: Cyber Hacking

Computer hacking is when someone modifies computer hardware or software in a way that alters the creator's original intent. People who hack computers are known as hacker's. Hackers are usually real technology buffs who enjoy learning all they can about computers and how they work.

This chapter explains about hackers'-nature and character, hackers' culture, possible ways of hacking, hackers' group, changing nature of hackers' culture, cracking, phreaking and hacking, hackers' behaviour, cyber hacking in UK, cyber hacking in India.

Chapter 2: Cyber Fraud

Computer Crime refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target net crime refers to criminal exploitation of the Internet.

This chapter explains about the Cyber Fraud, possible modes of Cyber Fraud, Cyber Fraud by false representation, Cyber lottery fraud, electronic-mail fraud and internet fraud, socio-legal impact of Cyber Fraud in India.

Chapter 3: Cyber Pornography

Cyber Pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyber pornography is a criminal offence, classified as causing harm to persons.

This chapter explains about the International initiatives to combat Cyber Pornography, Cyber Pornography in the UK, prevention and control of Cyber Pornography in India. Legislative approach in India to prevent and control Cyber Pornography.

Chapter 4: Cyber Crime

Cyber Crime encompasses any criminal act dealing with computers and networks (called Hacking). Additionally, Cyber Crime also includes traditional crimes conducted through the Internet.

This chapter mainly explains about the meaning of Cyber Crime, what is a Cyber Crime, Cyber Warfare, elementary problems associated with Cyber Crimes, legal protection against Cyber Crime in India. Other online frauds and financial crises, prevention methods to Cyber Crimes, preventive steps for organization and Government, problems related with Cyber Crime, case studies, types of Cyber Crime, tools used for Cyber Crime, other Cyber Crime methods and connections between terrorism and Cyber Crime.

Chapter 5: Cyber Crime and Punishment

Cyber Crime is a type of crime that not only destroys the security system of a country but also its financial system. One supporter of legislation against Cyber Crime states, “Our mouse can be just as dangerous as a bullet or a bomb”. Cyber attackers should be penalized and punishes severely and most Cyber Crimes have penalties reflecting the severity of the crime committed. Although in the past many laws against Cyber Crimes were insufficient, law enforcement agencies and Governments have recently proposed many innovative plans for fighting Cyber Crimes.

This chapter explains different types of Cyber Crimes, effective law enforcement, poor information security reduces the competitiveness of Nation, miscellaneous, weak penalties limit deterrence’s.

Chapter 6: Investigation of Computer Crime

This proliferation of crime involving computers has led to a need for specialties trained in the field of computer forensics, the scientific analysis of communication and data on computer storage devices. Specialties in computer forensics unite technical expertise with investigating skills and legal knowledge, a combination which is essential for computer crime investigation.

This chapter explains about the anonymity of cyberspace, cognizable & non-cognizable case, development of technology in India, investigation of Cyber Crime, lack of expertise, lack of sensitivity, legal framework, local jurisdiction, mechanism for online surveillance search and seizure, search warrant and special investigation.

Chapter 7: Cyber Terrorism and Cyber Attack

Cyber terror is now the new language of war that we understand only vagules. We know that more and more of our daily lives resolve around a digital world on the internet, our computer and our cell phones. Expect that the providers who sell us those digital services are taking steps to protect it against cyber attacks and we expect that the government is doing the same. But, experts warn us now that real danger is just around the corner if our government and businesses are not able to create a strong defence against Cyber attacks.

The terms “Cyber war” and “Cyber terrorism” have been extensively used in the media, in the official government reports and amongst academics. Even if they have been often hypes, experts agree that it is unlikely that cyber war will occur in the future.

This chapter explains about the Cyber Terrorism, evolution of Cyber Terrorism, attacks on National Security, International cyber attacks, Digital signature system, Cyber theft, Success of cyber threat, Errors in new software products, Inadequate resources, International convention on cybercrime, Growth in technical capabilities of terrorists, Improving security of commercial software, Education and awareness of cyber threats, Coordination between private sector and government, Cyber terrorism in India, Prevention and control of cyber terrorism in India.

Chapter 8: Evidentiary Value of a Videoconferencing

To provide the conference between two or more participants at different sites by using computer network to transmit audio and video data is called video conferencing.

This chapter explains clear definition of video conferencing. It explains benefits of video conferencing, methods of video conferencing, and major utilities of video conferencing.

Chapter 9: Internet

Internet is nothing but a global communication network that allows computer worldwide to connect and exchange information. It connects approximately 80 million users in Asian countries on any given data.

This chapter explains about concepts of internet, denial of access/denial of service, inception of computers and increasing use of internet. Obscenity and free expression human rights features and protection of minors.

Chapter 10: Mobile Phone, Privacy and Surveillance

Mobile phone, a telephone with access to a cellular radio system so it can be used over a wide area, without a physical connection to a network.

This chapter explains about history of mobile software development, Android application framework, developing Android application, applications of operating system user's designing the Android handsets, commonly used packages, how mobile phone networks works, open handset alliance and access to stored information on mobile phone sets.

Chapter 11: E-Commerce

E-Commerce stands for Electronic Commerce and caters to trading in goods and services through electronic medium such as internet mobile or any other computer network.

This chapter explains about the E-payment/Electronic payment gateways, payment gateways in India. Security issues including hacking, skimming, Identity theft, Phishing, Pharming, Taxation of E-Commerce and Foreign investment in E-Commerce.

Chapter 12: Cloud Computing

Cloud Computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the internet).

This chapter explains about the introduction to the Cloud Computing, Types of Clouds, Service Models, Cloud Computing in India and Cloud Computing and Cyber Crime.

Chapter 13: Digital footprints — Assessing Computer Evidence

On the Internet a digital footprints is the word used to describe that trial traces of "foot prints" that people leave online. This is information transmitted online such as forum registration, e-mails, and attachments, uploading videos or digital images and any other form of transmission of information — all of which leaves traces of personal information about yourself available to others online.

This chapter explains about computer evidence, the growth of computer forensics, personal computers, distributed processing, networking, internet, common computer forensic techniques and public policy issues.

Chapter 14: E-Mail Security

Electronic mail (also known as email or e-mail) is one of the most commonly used services on the internet, allowing people to send messages to one or more recipients. Cyber Criminals are motivated by financial gain, the challenge, ideology or simply mischief. So the anti-spam and virus filter from Spam Experts is a "must have" for any email intensive organization today.

This chapter explains about E-mail content filtering, E-mail retention, user training, E-mail encryption.

Chapter 15: National Cyber Security Policy — 2013

National Cyber Security Policy aims at protection of information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation. The objective of this policy in broad terms is to create a secure cyberspace ecosystem and strengthen the regulatory framework.

This chapter explains about Preamble, Vision, Mission, Objectives, Strategies, Creating a Secure Cyber Ecosystem, Creating an assurance framework, Encouraging open Standards, Strengthening the Regulatory framework, Creating mechanisms for Security threat early warning, Vulnerability management and response to security threats, Securing E-Governance Services, Protection and Resilience of Critical Information Infrastructure, Promotion of Research & Development in Cyber Security, Reducing supply chain risks, Human Resource Development, Creating Cyber Security Awareness, Developing effective public private partnership, Information sharing and cooperation, Prioritized approach for implementation, Operationalisation of the policy.

(Dr. S. Amar Prasad Reddy)
Additional Director-General
National Cyber Safety and Security Standards

Editorial Board

Highlights

40 +

Accolades

60 +
Case Studies

Abbreviations

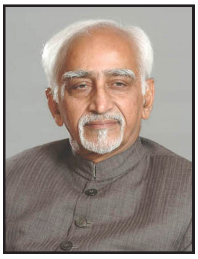
30 +
Diagrams

Glossary

Chapters

Accolades

सत्यमेव जयते



His Excellency

Mohammad Hamid Ansari

Vice President of India, New Delhi

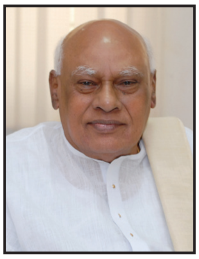
Honourable Vice President of India is happy to know that the National Cyber Safety & Security Standards, Chennai is publishing a book titled "National Cyber Crime Reference Handbook" focusing on the issues of Cyber Crime in the country.

The Vice President of India extends his greetings and good wishes to all those associated with the publication.

(Nagesh Singh)

Officer on Special Duty to the
Vice - President of India

सत्यमेव जयते



His Excellency

Dr. K. Rosaiah

Governor of Tamil Nadu

I am pleased to learn that the National Cyber Safety and Security Standards is launching the "National Cyber Crime Reference Handbook".

We are in the era of Information Technology and today Computers, Laptops and Internet have become a necessity and a household name in this fast developing technological world. Of late we see increase in Cyber Crimes. Prevention and control of Cyber Threats and Cyber Crimes are the need of the hour. Knowledge on adoption to Cyber Safety and Security is imperative.

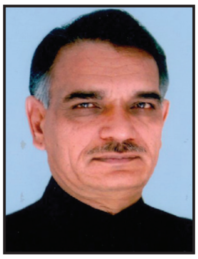
I congratulate the National Cyber Safety and Security Standards for their Initiatives to ensure Cyber Security.

I wish a successful launch of "National Cyber Crime Reference Handbook".

K. Rosai

(K. Rosaiah)

सत्यमेव जयते



His Excellency

Shivraj V. Patil

Governor of Punjab and Administrator
Union Territory, Chandigarh

I am happy to learn that the National Cyber Safety and Security Standards, Chennai is going to publish a Handbook "National Cyber Crime Reference Handbook", as a National Initiative to address the present issues on Cyber Crime.

A Cyber Crime is any crime that involves a computer and a network. It includes traditional crimes such as identity theft, internet fraud and credit card accounts thefts. Such crimes are illegal and may threaten a Nation's financial health and security.

Preventing Cyber Crime is a big issue nowadays! And this Handbook will help in protecting our National Critical Infrastructure from malicious cyber threats.

I extend my best wishes to the organizers on this National Initiative and hope it comes out with positive results.

(Shivraj V. Patil)

सत्यमेव जयते

Her Excellency

Urmila Singh

Governor of Himachal Pradesh

It gives me immense pleasure to learn that **National Cyber Safety and Security Standards** is publishing a book **National Cyber Crime Reference Handbook**.

The initiative is praiseworthy as Cyber Crime is an issue that concerns all and generating awareness about it is absolutely necessary.

I am glad that National Cyber Safety and Security Standards has taken up this task which would go a long way in addressing the issues related to Cyber Crime

I wish the endeavour great success.

(Urmila Singh)

सत्यमेव जयते

His Excellency

Vakkom Purushothaman

Governor of Mizoram

Initiative of publishing "National Cyber Crime Reference Handbook" is a praiseworthy attempt by National Cyber Safety and Security Standards. I congratulate the efforts of all those who conceived the idea and compiled various protection tools in the shape of a reference book.

While potentialities of cyber technology have proved to be of immense convenience, the problems of cyber technology pose imminent challenge. Cyber Crime is the emerging concern. In the world highly dependent on e-technology, all activities ranging from business to banking, commerce to communication are vulnerable to Cyber Crime. National Security can be strengthened best through knowledge of cyber security.

I am sure the Handbook would generate needed awareness and guarantee needed consciousness about security.

(Vakkom Purushothaman)

सत्यमेव जयते

His Excellency

Janaki Ballav Patnaik

Governor of Assam

I am glad to know that the National Cyber Safety & Security Standards is publishing a book, “National Cyber Crime Reference Handbook” as National Initiative to address the present issues on Cyber Crime. This is indeed a very timely effort and I am sure that this book would provide ample information on the various approaches, methods and means to curb and control the menace of Cyber Crime that is infesting every developed and developing Nation of the world.

The Cyber World has been created by computers and computer networks. The internet which is an electronic communications network that connects computer networks and organizational computer facilities around the world is an interactive tool for instant access of information and knowledge on nearly every subject. The web has created the super express highway of communication and infotainment connecting every part of the globe which, in turn, has made the concept of Global Village a virtual reality.

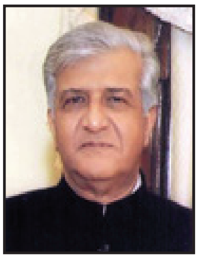
Cyber Crime is a crime involving computers and networks, where the computer may be used in committing the crime or it may also be its target. Such crimes, besides threatening a Nation’s Security and Financial Stability also create problems of privacy when confidential information is lost or intercepted, lawfully or unlawfully. Issues surrounding such crimes, particularly those relating to cracking, copyright infringement, child pornography and child grooming, have become serious concerns the world over.

Cyber tools when put to proper use can be as constructive as nuclear weapons can be destructive. But human history proves that there exist a certain kind of humans whose won't is to misuse or abuse nearly every instrument of human progress and development and it is these people with such distorted minds that have become the harbingers of Cyber Crimes.

I congratulate the National Cyber Safety & Security Standards for bringing out this invaluable handbook which would enable all to understand and prevent Cyber Crimes.

(Janaki Ballav Patnaik)

सत्यमेव जयते



His Excellency

Dr. K. K. Paul

Governor of Meghalaya

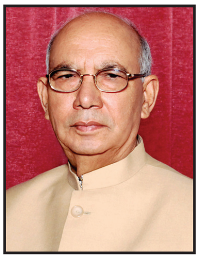
I am glad to learn that the National Cyber Safety and Security Standards, is publishing a "National Cyber Crime Reference Handbook" as a National Initiative to address the issues on Cyber Crime.

Cyber Crimes involve the use of Information Technology and networks. Issues surrounding these crimes are generally high profile involving financial theft, copyright, hacking, pornography etc. They can also have serious implications for National Security. The Initiative of the National Cyber Safety and Security Standards is therefore very timely and desirable.

I hope that the Reference Handbook will be of immense value to the investigating and intelligence agencies and others concerned with preventing and investigating Cyber Crimes and I wish the publications all success.

(K. K. Paul)

सत्यमेव जयते



His Excellency

H. R. Bhardwaj

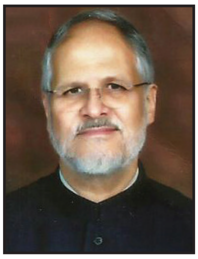
Governor of Karnataka

I am extremely happy to note that the **National Cyber Safety & Security Standards,** is publishing **"National Cyber Crime Reference Handbook"** comprising detailed perspective of the Cyber-Crimes which are creating massive trouble for India's National Security, in order to address the current issues on Cyber Crime by giving advanced protection methodologies and controlling procedures/tools, which will serve the Administrators, Judicial Authorities & Civil Servants to enhance their knowledge on Cyber Security.

I send my felicitations and best wishes to the publishers on this National Initiative.

(H. R. Bhardwaj)

सत्यमेव जयते



His Excellency

Najeeb Jung

Lieutenant Governor, Delhi

I am happy to learn that the National Cyber Safety & Security Standards, is publishing a book "National Cyber Crime Reference Handbook" as a National Initiative to address the present issues on Cyber Crime.

It is good note that the book will comprise the detailed perspective of the Cyber Crimes which are creating trouble for India's National Security and also that this book gives us advance cyber protection methodologies and controlling procedures/tools.

On this occasion, I wish all success for the publication of the book.

(Najeeb Jung)

सत्यमेव जयते

His Excellency

Shekhar Dutt SM

Governor of Chhattisgarh, Raipur

I am happy to learn that National Cyber Safety & Security Standards, is Publishing a book "National Cyber Crime Reference Handbook" as a National Initiative to address the present issues on Cyber Crime.

Cyber Crimes or computer-internet based crimes are becoming a big threat to our society, country and worldwide. We have to create awareness among people about various types of Cyber Crimes and take Safety and Security measures. I am confident this book will be very useful in this respect.

I convey my best wishes for the publication.

(Shekhar Dutt)

सत्यमेव जयते

His Excellency

Shriniwas Patil

Governor of Sikkim

It gives me immense pleasure to learn that **National Cyber Safety and Security Standards**, Chennai is going to publish a book **"National Cyber Crime Reference Hand-Book".**

The growth of the internet gave rise to many important services accessible to anyone with a connection. While malicious users often use the internet for personal gain, this may not be limited to financial, material gain. The use of the internet or other electronic means to harass an individual, a group of individuals, or an organization is increasing. It may include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, etc amounts to Cyber Crime.

The efforts of the Committee to issue the Handbook free of cost to all Ministries, Judicial Authorities, Government Departments of Central and State including Police, National Libraries all over the country deserve appreciation.

I hope the handbook will be of immense use and will be of great reference provider to curb Cyber Crimes which are creating threats to India's National Security and also to society.

I convey my best wishes to the dedicated members of the National Cyber Safety and Security Standards for bringing out this Handbook.

S. Patil

(Shriniwas Patil)

सत्यमेव जयते

His Excellency

Jagannath Pahadia

Governor of Haryana, Chandigarh

I am pleased to know that National Cyber Safety and Security Standards, is going to bring out "National Cyber Crime Reference Handbook" with a view to generate awareness against Cyber Crime.

Today is the era of Information Technology, which is a leading component towards globalization. It has opened new opportunities for countries like India, which has maximum scientific and technical manpower in the world. But, on the other hand, it has appeared as a threat to National Security which is a matter of great concern today. The need of the hour is to achieve perfection in every sphere in order to face this massive problem.

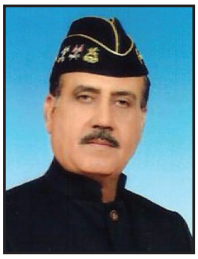
It is heartening that National Cyber Safety and Security Standards is devoted to promote advanced cyber protection methodologies and controlling procedures. I hope that the Handbook would prove a mile stone in this context.

I extend my best wishes for the successful publication of "National Cyber Crime Reference Handbook".

Jagannath Pahadia

(Jagannath Pahadia)

सत्यमेव जयते



His Excellency

Lt.Gen (Retd) A. K. Singh

Lieutenant Governor, Andaman & Nicobar Islands

I am happy to note that National Cyber Safety and Security Standards is bringing out a “National Cyber Crime Reference Handbook” to address the present issues on Cyber Crime.

Cyber Crime presents a tough challenge to all law enforcement agencies in this ever changing environment. These law enforcement agencies need to continuously update their skills and upgrade technology to counter this threat effectively. This is imperative in order to provide a secure cyber echo system in the country which will generate trust and confidence in IP system and transactions in cyberspace, thereby enhancing adoption of IT in all sectors of the economy.

I wish the National Cyber Safety and Security Standards every success in their endeavour to build a secure and resilient Cyberspace for citizens, business and Government.

(A. K. Singh)

सत्यमेव जयते

Shri. **Oscar Fernandes**

Honourable Minister for Road Transport & Highways

Government of India

I am happy to hear that National Cyber Safety and Security Standards is launching the "National Cyber Crime Reference Handbook" for providing a safe platform to the cyber world in India. Our mother land is enriched with a lot of potential human resources and our young generation proved that we can lead the global information technology arena.

Hope your effort will give a boost to the Government and Private Sector and in turn our children studying in schools and colleges and the citizens and technologies will get protected in the long run.

I wish the National Cyber Safety and Security Standards every success in their endeavours.

(Oscar Fernandes)

सत्यमेव जयते

Shri. **Beni Prasad Verma**

Honourable Minister of Steel

Government of India

It gives me immense pleasure to know that the National Cyber Safety and Security Standards, is publishing a book "National Cyber Crime Reference Handbook" for Central/State Government Ministries/Departments to enhance their knowledge on Cyber Security.

In this era of information revolution, Cyber Crimes are creating massive trouble for National Security. Knowledge of cyber protection methodologies and controlling procedures/tools is essential for every individual to cope with these security threats. I hope the Handbook would be very useful for security agencies.

I extend my best wishes for successful publication of this Handbook.

(Beni Prasad Verma)

सत्यमेव जयते

Dr. Kavuru Sambasiva Rao

Honourable Minister of Textiles
Government of India

The National Cyber Safety & Security Standards is launching the "National Cyber Crime Reference Handbook" as part of their National Initiatives. In implementing of its responsibilities towards the Nation, the National Cyber Safety and Security Standards is bringing good reference material for National Cyber Security Issues. It will help the stakeholders from Government Sectors and Industrial Organizations to prevent their Critical Infrastructure from malicious cyber threats. We hope that, this book will play an important role in current developments that are taking place in Cyber Security. I wish the National Cyber Safety and Security Standards, its whole Staff, all success in their future accomplishments.

(K. S. Rao)

सत्यमेव जयते

Dr. M. Veerappa Moily

Honourable Minister of Petroleum & Natural Gas
Government of India

I am glad to know that the National Cyber Safety and Security Standards, is bringing out a book "National Cyber Crime Reference Handbook" to address the present issues on Cyber Crime.

As conveyed to me that this book will comprise the detailed perspective of the Cyber-Crimes which are creating massive trouble for India's National Security and also this book gives advanced cyber protection methodologies and controlling procedures/ tools. I avail this opportunity to convey my sincere thanks for the painstaking efforts in bringing out this book in such an excellent form.

I am sure that the book with all these unique features will pander to the needs of readers.

My best wishes for success of this book.

(M. Veerappa Moily)

सत्यमेव जयते

Shri. **Narendra Modi**
Honourable Chief Minister
Gujarat

Starting from the Stone Age, it has always been human psyche to protect itself from external threats. The ideas, tricks and the methodology of protection from evil and intruding threat factors have also evolved over the time. Initially we, the humans, had to guard ourselves from physical threats like invaders and the **looters**. Nowadays, with the rising popularity of cyber connectivity and worldwide interlinking, the evil has also evolved in the form of **breach** of cyber security. It is a virtual world we have created and we have to be well prepared to protect and sustain our virtual world from the virtual invaders.

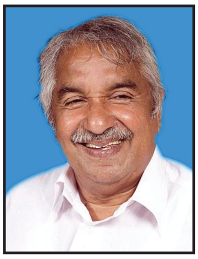
I am really happy to learn that the **National Cyber Safety & Security Standards** is thinking about the possible solutions and establishing norms against Cyber Crimes by the means of publication of **National Cyber Crime Reference Handbook**. It is also appreciable that the Institution is also going to give it free of charge to all the **Government Agencies** dealing with the issue.

I hope the Handbook will establish and convey the most effective ways and means of protecting our National Security against the worst sort of cyber attacks and provide the best safe guards against the cyber criminals threatening our Nation and its Integrity.

I wish all the success to the **National Cyber Safety and Security Standards** in its crusade to protect the Nation.

(Narendra Modi)

सत्यमेव जयते



Shri. **Oommen Chandy**
Honourable Chief Minister
Kerala

I am glad to know that National Cyber Safety & Security Standards, would be publishing a Reference Handbook on "Cyber Crime".

My hearty congratulations to all associated with National Cyber Safety & Security Standards for coming up with an informative handbook on Cyber Crimes, especially in the wake of the country going through increasing forms of the same. I hope that the Initiatives of National Cyber Safety & Security Standards in the domain of Cyber Crimes would go a long way in securing the country from the menaces of Cyber related crimes.

Wishing all success.

(Oommen Chandy)

सत्यमेव जयते

Shri. **Neiphiu Rio**
Honourable Chief Minister,
Nagaland, Kohima

I am happy to know that the National Cyber Safety and Security Standards (an Autonomous Body undertaken by National Cyber Safety Ltd) is publishing a book "National Cyber Crime Reference Handbook" as a National Initiative to address the present issues of Cyber Crime, and to distribute the book free of cost for the Central/ State Government Departments, Police Departments and National Libraries etc all over the country.

The publication of such a Handbook is a timely and welcome initiative. With internet becoming an essential part of our life, our culture and our work, and with our ever increasing dependence on the internet and other computer soft-ware programs for running most of our offices – whether Government, corporate or private offices, there is a looming threat or danger of it being used by enemy countries or by terrorists to sabotage the system, and wreck havoc on our life and our economy. There is a real possibility of all our banking services, our transport and communication systems, our power management systems etc being sabotaged by our enemies that can paralyze our life and our economy. Hence the importance of Cyber Security, which is a relatively new subject, cannot be over emphasized, and the publication of the Handbook will go a long way in making us better prepared to protect ourselves from such dangers and eventualities.

I wish the publication a grand success.

04/10

(Neiphiu Rio)

सत्यमेव जयते

Shri. **Ashok Gehlot**

Honourable Former Chief Minister

Rajasthan

I am glad to know that National Cyber Safety & Security Standards is publishing a book titled "National Cyber Crime Reference Handbook".

Today internet, websites and social sites have become preferred means of communication. However, the emergence of Cyber Crime has posed serious challenges to our Security System. It is also a big course of concern for the security agencies and the Governments across the globe.

I hope that the Handbook will carry information about the Cyber Crimes which are posting a threat to the National Security while providing methodologies and procedures for effective control of Cyber Crimes.

I send my good wishes for the success of the endeavour.

(Ashok Gehlot)

सत्यमेव जयते

Shri. **Paban Singh Ghatowar**

Honourable Minister of State (Independent Charge)
Ministry of Development of North Eastern Region and
Minister of State for Parliamentary Affairs
Government of India

I am extremely happy to know that **National Cyber Safety & Security Standards** is publishing **"National Cyber Crime Reference Handbook"**, to address the issue of Cyber Crime. I am sure that this National Initiative captures detailed perspective of Cyber-Crimes which poses a massive challenge for National as well as Global Security. I am confident, the handbook will act as the repository of collection wisdom on advanced cyber protection methodologies and controlling procedures.

Today the cyber-world has reached its pinnacle in the history of mankind. The world has shrunk into a global village but, as it always happens, the cyber world also presents a humongous drawback of being misused and spreading undesirable contents.

The Cyber Crime grows beyond the national boundary and thus regions like North Eastern India with 96% international boundary, becomes a prime concern from safety and security points of view.

Deterring Cyber Crime is an integral component of National Cyber Security and critical information infrastructure protection strategy. At the Nation level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of Government Authorities, the private sector and citizens.

I convey my best wishes for a successful release of National Cyber Crime Reference Handbook.

(Paban Singh Ghatowar)

सत्यमेव जयते

Prof. K. V. Thomas

Honourable Minister of State (Independent Charge)
For Consumer Affairs, Food & Public Distribution
Government of India

I am very happy to learn that the National Cyber Safety & Security Standards is publishing a book "National Cyber Crime Reference Handbook", which will act as a reference material for administrative and judicial authorities in India to be able to tackle Cyber Crimes in a better and efficient manner.

Cyber Crime, a criminal activity committed with computer and/or over a network or the internet affects not just the people who have been taken for a ride by cyber criminals, but the economy of a country as well. This has a huge impact on growing economies of the world like India, which has been increasingly using internet for a wide variety of business purposes.

Publication of the National Cyber Crime Reference Handbook is a good initiative in the right direction in guiding administration in India on how to go about tackling the menace of Cyber Crime. I convey my best wishes to the National Cyber Safety and Security Standards on its proactive efforts in bringing out such an invaluable tool in the hands of law of enforcing agencies and hope that it will continue its efforts in fighting Cyber Crime in every ingenious way possible.

I wish the National Cyber Safety and Security Standards success in all its future endeavours.

(K. V. Thomas)

सत्यमेव जयते

Shri. **Manikrao Gavit**

Honourable Minister of State for Social Justice and Empowerment

Government of India

I am delighted to know that **National Cyber Safety and Security Standards** is launching a **"National Cyber Crime Reference Handbook"** to protect our National Critical Infrastructure from malicious cyber threats.

In the contemporary times, when the business of Government and public sector undertakings is conducted on-line, there is always looming threat of invasion hacking by criminals. I hope that, this book will address the recent developments that are taking place towards Cyber Defence.

The Ministry of Social justice and Empowerment is happy to participate and support this National Initiative. I wish all success to **National Cyber Safety and Security Standards** and its staff, in their future endeavours.

(Manikrao Gavit)

सत्यमेव जयते

Smt. **Panabaka Lakshmi**

Honourable Minister of State for
Petroleum and Natural Gas & Textiles
Government of India

I am happy to learn that the National Cyber Safety and Security Standards, is bringing out a book "National Cyber Crime Reference Handbook" to address the present issues on Cyber Crime.

As mentioned to me that this book will comprise the detailed perspective of the cyber-crimes which are creating massive trouble for India's National Security. This book also gives us advanced cyber protection methodologies and controlling procedures/tools. I take this opportunity to convey my sincere thanks for the endeavour in publishing this valuable book.

I am sure that the book with all these unique features will pander to the need of readers.

My best wishes for success of this book.

Panabaka Lakshmi

(Panabaka Lakshmi)

सत्यमेव जयते

Dr. D. Purandeswari

Honourable Minister of State for Commerce & Industry
Government of India

I am happy to learn that the National Cyber Safety and Security Standards, is launching the "National Cyber Crime Reference Handbook" as part of their National Initiative Schemes. In execution of its responsibilities, the National Cyber Safety and Security Standards is bringing this important reference material for National Cyber Security Issues. It will help the Stakeholders from Government to Industry to prevent their critical infrastructure from cyber threats. In general, this book will address the recent developments that are taking place towards Cyber Defence. The Ministry of Commerce & Industry is happy to participate and support this National Initiative as an Institutional Partner.

I wish the National Cyber Safety and Security Standards all success in their endeavours of outreach through this National Initiative, which I am told would be published on yearly basis.

(D. Purandeswari)

सत्यमेव जयते

Shri. **Rajeev Shukla**
Honourable Minister of State for
Parliamentary Affairs & Planning
Government of India

I am delighted to know that National Cyber Safety and Security Standards is bringing a "National Cyber Crime Reference Handbook" to protect our National Critical Infrastructure from malicious cyber threats.

This National Initiative will be a great effort to enlighten the Government sectors, Public and Private industries and Academic Institutions towards the Cyber Security domain.

I believe it will be very helpful to strengthen the National Cyber Security Policy. My best wishes to National Cyber Safety and Security Standards on this National Initiative and hope it comes out with more such positive ideas.

(Rajeev Shukla)

GOVERNMENT OF TAMIL NADU

TRUTH ALONE TRIUMPHS

Honourable **Mr. Justice R. K. Agrawal**

Chief Justice, High Court of Madras

One of the biggest Challenges which India faces is Cyber Crime. Our dependence on Computers is such that even a moment's disruption of computer networks will have a cascading effect on our regular routines. This has led to spurt of a new sort of crime which is called Cybercrime. Some of them are spams, hacking, computer frauds, posting obscene contents in websites and Cyber Stalking etc Apart from these, Cyber terrorism poses big threat to National Security.

I am happy to note that National Cyber Safety and Security Standards, is bringing out a book, to be distributed free of cost to the various stakeholders viz., Central/State Government Departments/Police Departments/National Libraries all over the Country, Comprising the detailed perspective of the Cybercrime and advanced Cyber protection methodologies and controlling procedures/tools. I hope this book will be highly useful as a reference material for various Authorities and also enhance them with greater Knowledge on Cyber Security.

I Congratulate National Cyber Safety and Security Standards for their Initiative and wish them every success.

RKAgrawal

(R. K. Agrawal)

सत्यमेव जयते

Honourable **Mr. Justice Barin Ghosh**

Chief Justice, High Court of Uttarakhand

I am happy to learn that National Cyber Safety & Security Standards, is coming out with a publication “National Cyber Crime Reference Handbook”, containing therein detailed material to understand Cyber–Crimes as well as higher Cyber–Crime protection methods and controlling measures, which is intended to be issued free of cost for the Central/State Government departments/National libraries all over the country. I hope and trust that the book, having the projected reading materials will be extremely useful to deal with all such type of Cyber–Crime problems and also to know about safety methods and controlling measures in the matter. I hope and trust that the Institute will up keep the information in future also.

I wish all the success to the publication.

(Barin Ghosh)

सत्यमेव जयते

Honourable **Justice Dr. Manjula Chellur**
Chief Justice, High Court of Kerala

The Publication of a book on **"National Cyber Crime Reference Handbook"** is a laudable exercise which would give an insight on many issues. Especially the safety measures and other protection mechanisms so far as Cyber Crimes are concerned. The contents of this book would not only create awareness on the subject matter but also assist various departments so far as knowledge on Cyber Security and related matters.

I congratulate the organizers on this venture.

C. Manjula

(Manjula Chellur)

सत्यमेव जयते

Honourable **Mr. Justice Sanjay Kishan Kaul**

Chief Justice, High Court of Punjab & Haryana

I am Happy to know that the **National Cyber Safety & Security Standards**, is Publishing a book, **"National Cyber Crime Reference Handbook."**

Internet with its varied benefits also causes serious challenges in myriad ways. This causes both a security threat and affects the social fabric. Cyber Crime is, thus, an off shoot of this new cyber world. In order to detect and protect against Cyber Crime, a different approach in law becomes necessary.

The Reference Handbook being a compilation would provide the necessary assistance and knowledge for cyber protection methodologies and tools, both for the legal fraternity and the common man.

I am sure that this book will receive great acceptance and I convey my best wishes to all.

(Sanjay Kishan Kaul)

सत्यमेव जयते

Honourable **Justice Rekha M. Doshit**
Chief Justice, High Court of Patna

I am pleased to note that the National Cyber Safety and Security Standards has decided to publish "National Cyber Crime Reference Handbook". I am sure the Handbook will be a valuable addition to any Library, particularly for the netizens.

In the present day of Information Technology, no one can afford to be net ignorant. One may not be net savvy or a netizen, still no body is spared of the wingspan of the net activities.

Every one of us has, at some point of time, been the victim of Cyber Crime. At times the damage is imperceptible and the victim is not even aware that he is targeted. The most common of imperceptible Cyber Crimes is hacking of the E-mail address.

I believe your book will be of great help to the netizens and to the Computer illiterate people equally. I wish your book a great success.

(Rekha M. Doshit)

सत्यमेव जयते

Honourable **Mr. Justice A. M. Khanwilkar**
Chief Justice, High Court of Himachal Pradesh

I am glad to pen this prelusory message on the occasion of publication of "National Cyber Crime Reference Handbook". This book disseminates information on scarcely treaded path. The information available in this book is both instructive and educative. It would not only help the members of legal profession but also other duty holders expected to unravel the dubious techniques resorted to by miscreants and including to the National Security. In the contemporary times, when the business of Government and public sector undertakings is conducted on-line, there is always looming threat of invasion/hacking by criminals and anti national elements. This book has provided insight into the techniques which can frustrate and preempt such attempts. The work of this nature elevates the standards to safeguard website from invasion and intrusion, by miscreants and it also immaculately spells out the prescription for detection of Cyber Crime. I welcome the publication of this book and extend my best wishes for the success of the same.

(A. M. Khanwilkar)

सत्यमेव जयते

Honourable **Justice Dr. P. Jyothimani**

Former Judge, Madras High Court

Advisor - National Cyber Safety and Security Standards

Now-a-days, the use of computer and internet has become inevitable. Where there is an invention or development of any kind in the society, there is a room for the misuse, though the range and ambit of misuse may differ depending on the nature of invention or development.

The cyber field is not an exception. The policy maker has to keep the issue pattern before drafting policies and the Government of India has to come with Special Cyber Courts to handle the Cyber Crime Cases.

I congratulate the National Cyber Safety and Security Standards on bringing out this edition of "National Cyber Crime Reference Handbook". I am sure this publication will help to enhance the knowledge and skill to protect one and all from Cyber Crime.

I wish the publication a huge success.

(P. Jyothimani)

Smt. Rinchen Ongmu, I.A.S.,

Chief Secretary, Government of Sikkim, Gangtok

With the wide spread use of computers and internet, "Cyber Crime" has emerged as a major challenge for law enforcement agencies around the world. Anyone who uses the internet and other online technologies extensively can fall victim to Cyber Crime.

The "National Cyber Crime Reference Handbook" is a National Initiative to address the present day issues on Cyber Crime. This book gives an insight into the types of Cyber Crime which are not only posing threat to the National Security, but also gives rise to economic offences due to the ever increasing use of online banking, e-Commerce, etc.

The Government of Sikkim has taken all initiatives to address the threat posed by Cyber Crime to our information system. Measures are afloat to combat this menace by creation of a Cyber Forensic Laboratory. Cyber Cafe Rules have been formulated preventing misuse of the Cyberspace especially through social media.

I congratulate the National Cyber Safety and Security Standards on bringing out this edition of "National Cyber Crime Reference Handbook". I am sure this publication will be of immense value and will help to enhance the knowledge and skill to protect one and all from Cyber Crime.

I wish the publication a huge success.

6/11/13

(Rinchen Ongmu)

सत्यमेव जयते

Shri. **Sudripta Roy**

Addl. Chief Secretary, Himachal Pradesh

In the last two decades we have made rapid progress on the technology front. While the primary goal of such progress is the improvement in the lives of the citizens and raising the basic levels of social services, we cannot be ignorant of the fact that the increase in sophistication of technology also endangers our daily lives. In today's digital age there are no physical boundaries and the individuals, corporate and Governments face increased risks in becoming targets of Cyber-attacks. Internet, though offering great benefit to society, also present opportunities for crimes using new and highly sophisticated technological tools. With increasing internet and mobile penetration in a country like India, the incidents of such Cyber-Crimes are likely to increase over the coming years.

The primary targets of Cyber-attacks are critical infrastructures such as financial and utility systems. Government websites and corporations, producing effects that are similar to terrorist attacks in the physical space. While increased security measures are definitely helpful, it is essential to spread the awareness regarding the potential risks of using the shared internet infrastructure. Cyber Security needs to be implemented and enhanced across all organizations and all the employees need to be trained on the same. With this objective this "National Cyber Crime Reference Handbook" will serve as a reference for various departments of the Government of Himachal Pradesh. We hope that the users will be able to navigate through the various aspects of Cyber Security, and this in turn will help in preventing the Cyber-attacks in the future.

Special Secretary (IT) to the
Governement of Himachal Pradesh

सत्यमेव जयते

Shri. **G. A. Rajkumar, I. A. S.**
Former Additional Chief Secretary to Government
Chairman, National Executive Committee,
National Cyber Safety and Security Standards

I am glad to note that a National Cyber Safety and Security standards is publishing a "National Cyber Crime Reference Handbook."

National Cyber Safety and Security is a key aspect to our mother land India's Social Security and Defence. In spite of this fact, Anti National elements are doing their best in the Cyber World to spoil our National heritage and social values of our citizens, and trying to disturb our National Unity. Now it is the duty of all citizens and organizations to visualize and identify innovative measures for Cyber Safety.

I strongly believe that this Initiative will bring a great success to National Cyber Safety and Security Standards and I wish all success in their future endeavours.

Rajkumar

(G. A. Rajkumar)

सत्यमेव जयते

Shri. **Satish Chandra Tewary, I.A.S.**

Former Principal Secretary to the Government of West Bengal

Digital technology and internet is increasingly becoming an integral part of present day existence. The young generation prefer to text, tweet, and post their daily lives in social media. People irrespective of age prefer plastic over cash. More and more services of the Government are being delivered on-line obviating the need for the citizen to visit the respective Government offices. However, the same internet and automated data systems also present an enormous new threat for criminal activity. Computers and other electronic devices are being used increasingly to commit, enable, or support crimes perpetrated against persons, organizations or property. Every day, public investigating officers, Adjudicate Departments and public prosecutors come across cases where offences in some kind or other in the digital world are involved. Both the west Bengal police and Kolkata police have separate cells to deal with the growing menace of cyber offences.

It is heartening to note that **National Cyber Safety and Security Standards,** has taken a timely initiative to publish the **National Cyber Crime Reference Handbook**. This handbook illustriously points out various forms of serious and complex Cyber Crimes plaguing the cyber environment and charts out means to cope up and stave off the potential threats from new tech savvy law breakers.

I am very pleased and thankful to the authors and experts for their contributions to this handbook and will recommend it to all incumbent government departments, police departments in the state to enhance their understandings on cyber security and Cyber Crime.

S.C. Tewary 22.10.2013

(Satish Chandra Tewary)

Shri. **Ashok Prasad, I. P. S.,**

Director General of Police, Jammu & Kashmir

I am indeed delighted to know that the **National Cyber Safety & Security Standards,** has published the **"National Cyber Crime Reference Handbook".**

The handbook provides detailed insight into the menace of Cyber Crime and provides a comprehensive perspective on this vital issue. It is acknowledged world-wide that Cyber Crimes and associated activity in cyberspace have significant implications for National Security as well as economic and social stability. The enormous effort which has gone into the compilation of advanced Cyber Defence methodologies and controlling procedures/ tools is highly commendable.

I wish the members of the committee best of luck in their endeavour to publish such an informative book on Cyber Crime/Cyber Security.

(Ashok Prasad)

सत्यमेव जयते

Shri. **Besesayo Kezo, I. P. S.,**

Director General of Police, Nagaland, Kohima

I am happy to learn that the "National Cyber Safety and Security Standards", is publishing a book on Cyber Crime titled "National Cyber Crime Reference Handbook".

Cyber Crime is a recent phenomenon that poses potential dangers to every person due to the inter-connectedness of the world that we live in. Due to its recent origin, the law enforcement agencies are still in the process of evolving strategies to counter Cyber Crime. In such a context, this book is very timely and will enrich the existing literature on Cyber Crime. I am confident that this handbook will prove to be a useful tool to combat Cyber Crime.

(BESESAYO KEZO) IPS

15/10/13

(Besesayo Kezo)

Shri. **Nandan Dube, I. P. S.,**

Director General of Police, Madhya Pradesh

It gives me immense pleasure to know that **National Cyber Safety and Security Standards** is going to bring out **"National Cyber Crime Reference Handbook"** to provide information about National Cyber Security and its recent developments along with methodologies for prevention and control mechanisms of cyber threats.

The rapid and dramatic advances in information technology in recent years have generated tremendous benefits. It had also created significant and unprecedented risks with implementation. Computer security has thus become more important at all levels of an organization to avoid data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive information.

It is in this context that this Handbook will come handy for Cyber Security awareness not only in the Governments Sectors and PSU's but also in other industrial organizations.

I would like to congratulate **National Cyber Safety and Security Standards**, for this great effort and wish them all the best in their future endeavours.

(Nandan Dube)

Shri. **Prakash Mishra, I. P. S.,**

Director General of Police, Odisha

"Cyber Crime does not respect geographical location; it knows no boundaries, religion or nationality. Cyber criminals attack and spread across the whole world in a matter of minutes, sparing no one. The internet has made it easier to perpetrate crimes by providing criminals an avenue for launching attacks with relative anonymity. The increased complexity of the communication and networking infrastructure is making investigation of the Cyber Crimes difficult. Clues of illegal activities are often buried in large volumes of data that needs to be shifted through in order to detect crimes and collect evidence. The field of digital forensics and cybercrime investigation has become very important for law enforcement, national security, and information assurance. This is a multidisciplinary area that encompasses law, computer science, finance, telecommunications, data analytics, and policing. To investigate and prosecute Cyber Crime, law enforcement agencies need skilled investigators, up-to-date computer forensic examiners and prosecutors with Cyber Crime familiarity.

I am happy to note that, **National Cyber Safety & Security Standards** is publishing a book **"National Cyber Crime Reference Handbook"** as a National Initiative to address the present crimes on Cyber Crime. I am sure this book will be a great help to law enforcement agencies and will contribute to enhance Cyber Safety".

(Prakash Mishra)

Shri. **Shriniwas Vashisht, I. P. S.,**
Director General of Police, Haryana

Cyber Crime continues to show different facets with each day that passes. Cyber criminals are always finding new ways of organizing themselves and targeting new users and new platforms. On line transaction-based activities continue to be the most exploited, and hactivism related attacks continue to rise as way to commit corporate espionage, push particular agendas or cause reputational damage. In short, it is the new challenge for law enforcement, pursuit of which is going to take considerable effort.

I sincerely hope that this handbook will be useful to its readers, especially those engaged in the law enforcement. I need to record my appreciation for those who have made this compilation possible. I am happy to note that this handbook aims to give us knowledge about advanced cyber protection methodologies and tools. The present publication examines in detail the legalities of safeguards against Cyber Crime and provides a useful profile of the technology and counter-technology to give effect to cyber laws. I hope that this collection of focuses papers on cyber laws will provide all those working on the internet and in the area of Information Technology a valuable guide and reference work.

25/9/2013

(Shriniwas Vashisht)

MLP

MEGHALAYA POLICE

Shri. **PJ. P. Hanaman, I. P. S.,**

Director General of Police, Meghalaya, Shillong

I am, indeed, very happy to know that the National Cyber Safety & Security Standards, publishing a book, “National Cyber Crime Reference Handbook” that would cover a wide range of issues governing Cyber Crime with a primary focus on law enforcement.

Law enforcement agencies are today faced with hitherto unknown complex forms of Cyber Crime and Cyber Security. The common man’s dependence, as well that of the public institutions and services, on internet is increasing by the day and all aspects of our daily life have come to be immensely influenced by the use of the internet.

The unprecedented harnessing of the cyber facilities has naturally created unparalleled opportunities for criminals in this digital age to exploit and operate seamlessly and in most cases, without face and identity, across borders. Our vulnerabilities are very many.

It is in this context that the publication of such a Handbook assumes importance and I believe that such literature will help Law Enforcement Agencies in reinforcing their skill sets in dealing with Cyber Crimes.

I congratulate the organizers for this timely endeavour and excellent effort.

PJHanaman 19/11/2013

(PJ. P. Hanaman)

सत्यमेव जयते

Shri. **Ramniwas, I. P. S.,**

Director General & Inspector General of Police, Chhattisgarh

It gives me great pleasure to express a view for the Handbook to address the present issues on Cyber Crime. Information Technology (IT) has grown at breathtaking speed in the recent years. As result of the communication revolution, Cyberspace has become a virtual territory for the criminals to flourish. Computer Crime has been causing heavy losses to Government and businesses all over the world. The challenge, which the law enforcement agencies face today, however, is not just technological in nature but also has the legal, forensic and jurisdictional aspect.

I convey my heartiest congratulations to the authors and committee, I am sure that the book will give us advanced cyber protection methodologies and controlling procedures/tools and also provide a valuable insight to the police investigators, forensic scientists, security administrators, judiciary and to all those who may have to grapple with complexities of computer crime in the year to come. Due to communication technology world has become a global village.

My best wishes for the entire team.

30·11·2013.

(Ramniwas)

सत्यमेव जयते

Shri. **J. N. Choudhury, I. P. S.,**
Director General of Police
Assam, Ulubari, Guwahati

I am happy to know that the National Cyber Safety & Security Standards is publishing "National Cyber Crime Reference Handbook" and issuing the same. Free of cost to police departments and other Central/State departments. Its contribution towards clarifying issues related to Cyber Crime and Cyber Security will help evolve a set of global guidelines for the Investigating officers. Information Technology and the Internet had led to innovation, but have also created new avenues for mischievous elements to commit crimes in the Cyberspace. The possible misuse of this powerful technology by criminals requires a marching expertise in investigators by making them tech savvy and by appropriate response capabilities at the field level. As conventional investigation experience alone will not be sufficient to solve such complex technology crimes, the need for technical expertise is a must to address the problems faced by Government departments, banks, students and others, who become victim of Cyber Crimes. This Noble Initiative will go a long way in strengthening the National Security as well as in safeguarding the interest of individuals.

I extend appreciation to everyone involved in this venture.

(J. N. Choudhury)

Dr. S. S. Mantha

Chairman, All India Council for Technical Education
(A Statutory Body of the Govt. of India)

I am pleased to know that the National Cyber Safety and Security Standards, is launching the "National Cyber Crime Reference Handbook" to give information about the National Cyber Security, its recent developments which also provide the information about prevention and control of cyber threats. It will be beneficial to all the Stakeholders especially to the Government, Industry and to the Academic Institutions all over the Country. The AICTE is very happy to be an Institutional Partner to this National Initiative and I take this opportunity to extend my greetings to National Cyber Safety and Security Standards, its entire staff and wish them all success in this and all their future endeavours.

(S. S. Mantha)

Notes :

CONTENTS

CHAPTER 15 : NATIONAL CYBER SECURITY POLICY — 2013

Case Studies

Case Study 1: IIT Kharagpur, W.B., India (2002) Case

Case Study 2: Hacking in Baroda, Gujarat

Case Study 3: Hacker Dr. Neruker

Case Study 4: Delhi Hackers' Case

Case Study 5: Hackers "Phishing"

Case Study 6: Hacking between India and Pakistan

Case Study 7: Arrest of the Two Indian Computer Trainers at Chhattisgarh in 2001

Case Study 8: Arrest of Ex-Scientist in the Year 2001

Case Study 9: ATM Hacking

Case Study 10: Mobile Phone Hacking

Case Study 11: Mr. Bhardwaj Case, in the Year 2001

Case Study 12: Hacker Kalpesh Sharma's Case

Case Study 13: Online Traders Hacked

Case Study 14: Banks are Victims

Case Study 15: Pune Cyber Fraud Case

Case Study 16: Cyber Fraud in West Bengal

Case Study 17: Click Fraud

Case Study 18: Hyderabad Rs. 20 Crore Data Conversion Fraud

Case Study 19: Karan Bahree's Case

Case Study 20: Bangalore Cyber Fraud Case

Case Study 21: New Delhi Online Traders Case

Case Study 22: Bangalore Cyber Fraud, June 2006

Case Study 23: Kolkata Cyber Fraud Case, September 2006

Case Study 24: Lottery Fraud and Cyber Squatter

Case Study 25: Bobby Art International etc v Ompal Singh Hoon

Case Study 26: K.A. Abbas v Union of India

Case Study 27: Samaresh Bose v Mr. Amal Mitra

Case Study 28: Sukanto Halder v State of West Bengal

Case Study 29: Raj Kapoor v State of Maharashtra

Case Study 30: Mumbai Housewife Harassed due to Cyber Pornography 2003

Case Study 31: In Tamil Nadu v Suhas Katti

Case Study 32: A Man Posing as a 15 Year Old Girl

Case Study 33: Airforce BAL Bharti School 2001

Case Study 34: Bhubaneswar Case

Abbreviations

3G	Third Generations (Mobile Communication System)
ACMA	Australian Communications and Media Authority
AIAI	All India Association of Industries
AIC	Anti-Indian Crew
AIPAC	American Israel Public Affairs Committee
AMPS	Advanced Mobile Phone System
APIs	Application Programming Interfaces
ASL	Apache Software License
AT&T	American Telephone and Telegraph Company
ATM	Automated Teller Machine
AVS	Address Verification System
B2B	Business-to-Business
B2C	Business-to-Customer
BARC	Bhabha Atomic Research Centre
BPO	Business Processes Outsourcing
BPRD	Bureau for Paranormal Research and Defence
BSNL	Bharat Sanchar Nigam Limited
CAGR	Compounded Annual Growth Rate
CAIDA	Cooperative Association for Internet Data Analysis
CB	Citizens' Band
CBI	Central Bureau of Investigation
CCAOI	Cyber Cafe Association of India
CCIC	Cyber Crime Investigation Cell
CCPS	Cyber Crime Police Station
CCS	Central Crime Station
CD	Compact Disk
CDMA	Code Division Multiple Access
CDR	Call Data Record
CD-ROM	Compact Disc Read-Only Memory
CEO	Chief Executive Officer
CERT/CC	Computer Emergency Response Team /Coordination Centre
CID	Criminal Investigation Department
CNN	Cable News Network

CNP	Cardholder Not Present
COD	Cash On Delivery
COPS	Computer Oracle and Password System
COTS	Commercial-Off-The Shelf
CSI	Computer Security Institute
CSTARC	Cyber Security Tracking Analysis and Response Centre
CVV	Card Verification Value
CWIN	Cyber Warning and Information Network
D&B	Dun and Bradstreet
DD	Detective Department
DDOS	Distributed Denial-Of-Service
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DIT	Department of Information Technology
DNA	Deoxyribo Nucleic Acid
DOD	Department of Defence
DOS	Denial of Service
DOT	Department of Telecommunications
DPI	Deep Packet Inspection
DRDO	Defence Research and Development Organization
DRI	Direct Rendering Infrastructure
DSL	Digital Subscriber Line
EC	European Committee
ED	Election District
EDI	Electronic Data Interchanges
EEA	European Economic Area
ESN	Electronic Serial Number
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDI	Foreign Direct Investment
FIPB	Foreign Investment Promotion Board
FIR	First Information Report
FISMA	Federal Information Security Management Act
FSA	Financial Services Authority
FTP	Foreign Trade Policy

G8	Group of Eight
GILC	Global Internet Liberty Campaign
GPL	General Public License
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GTA	Grand Theft Auto
HDFC	Housing Development Fund Corporation
HERF	High Energy Radio Frequency
HEU	Hacking at the End of the Universe
HIP	Hacking in Progress
HTC	High Tech Computer
HTTPS	Hyper Text Transfer Protocol Secure
IaaS	Infrastructure-as-a-Service
IB	International Baccalaureate
ICANN	Internet Committee for Assigned Names and Numbers
ICOA	International Civil Organization for Aviation
ICT’s	Information and Communication Technologies
IDC	International Data Corporation
IDE	Integrated Development Environments
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
INL	Idaho National Laboratories
INR	Indian Rupee
IP	Internet Protocol
IPC	Indian Penal Code
IRC	Internet Relay Chat
ISACs	Information Sharing and Analysis Centres
ISE	Independent Security Evaluators
ISP	Internet Service Providers
IT	Information Technology
LAN	Local Area Network
LBS	Location-Based Services
LCD	Liquid Crystal Display
LOS	Lines of Site

LTS	Long Term Support
LTTE	Liberation Tigers of Tamil Eelam
MAC	Media Access Control
MEA	Ministry of External Affairs
MIN	Mobile Identification Number
MLA	Member of the Legislative Assembly
MLTA's	Mortgage Level Term Assurance
MMS	Multi-Media Message Services
MSPs	Mobile Service Providers
NASSCOM	National Association of Software and Service Companies
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NBC	Nuclear, Biological and Chemical
NCAS	National Cyber Alert System
NCMC	National Crisis Management Committee
NCSD	National Cyber Security Division
NDNC	National Do Not Call Registry
NDPS	Narcotic Drugs and Psychotropic Substances
NGO	Non Governmental Organization
NIC	National Informatics Centre
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NSP	Network Service Providers
NTT	Nippon Telegraph & Telephone Corporation
ODM	Original Design Manufacturer
OECD	Organization for Economic Co-operation and Development
OEM	Original Equipment Manufacturer
OHA	Open Handset Alliance
OMB	Office of Management and Budget
OSP	Other Service Provider
P2P	Peer-to-Peer
PaaS	Platform-as-a-Service
PACE	Police and Criminal Evidence Act
PAN	Permanent Account Number
PC	Personal Computer

PCI	Peripheral Component Interface
PE	Permanent Establishments
PHC	Pakistani Hackers' Club
PIL	Public Interest Litigation
PIN	Personal Identification Number
PMO	Prime Minister's Office
POTO	Prevention of Terrorism Ordinance
PRC	Peoples Republic of China
PSN	Public Switched Network
PTI	Press Trust of India
RAM	Random Access Memory
RBI	Reserve Bank of India
RDX	Research Department Explosive
RIPA	Regulation of Investigatory Powers Act
RTP	Real Time Protocol
SaaS	Software-as-a-Service
SATAN	Security Administrator's Tool for Analyzing Networks
SCADA	Supervisory Control and Data Acquisition
SDK	Software Development Kit
SDR	Special Drawing Right
SEBI	Securities and Exchange Board of India
SET	Secure Electronic Transactions
SGL	Simple Graphics Library
SIM	Subscriber Identity Module
SMS	Short Messaging Services
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Security Socket Layer
SSN	Social Security Number
TADA	Terrorist and Disruptive Activities Act
TAG	Technical Advisory Group
TDMA	Time Division Multiple Access
TDRS	Tracking and Data Relay Satellite
TD-SCDMA	Time Division Synchronous Code Division Multiple Access

TMSI	Temporary Mobile Subscriber Identity
TNIL	Techno Noble Info Way Ltd.
TRAI	Telecom Regulatory Authority of India
UCC	Unsolicited Commercial Communications
UCE	Unsolicited Commercial Emails
UDP	User Datagram Protocol
UFJ	United Financial of Japan
UI	Unique Identification Number
UIDA	Unique Identification Authority of India
UMTS	Universal Mobile Telecommunications System
UNCITRAL	United Nations Commission on International Trade Law
UNESCO	United Nations Educational, Scientific, and Cultural Organization
UNIX	Universal Network Information Exchange
URIs	Uniform Resource Identifiers
US-CERT	United States Computer Emergency Readiness Team
USD	United States Dollars
VISA	Vacation Insurance Savings Account
VM	Virtual Machine
VOIP	Voice over Internet Protocol
VPA	Virtual Payer Authentication
VSNL	Videsh Sancher Nigam Ltd.
WiMAX	Worldwide Interoperability for Microwave Access
WTC	World Trade Centre
WWW	World Wide Web
XML	Extensible Mark-up Language

अध्याय 1
Chapter 1
Cyber Hacking

Notes :

1.1 Introduction:

Computer hacking is when someone modifies computer hardware or software in a way that alters the creator's original intent. People who hack computers are known as hackers. Hackers think that what they do is like an art form. They usually have expert-level skills in one specific program. For most hackers, hacking gives them the opportunity to use their problem-solving skills and a chance to show off their abilities. Most of them do not wish to harm others.

The word "hacking" has two definitions. The first definition refers to the hobby/ profession of working with computers. The second definition refers to breaking into computer systems. While the first definition is older and is still used by many computer enthusiasts (who refer to cyber-criminals as "crackers"), the second definition is much more commonly used. In particular, the web pages here refer to "hackers" simply because our web-server logs show that everyone who reaches these pages are using the second definition as part of their search criteria.

What kind of Information can a Hacker Steal from my Computer?

Personal information, names address, financial information, even the account information for your ISP and passwords, in short anything stored on your computer can be obtained by a hacker. A Trojan may record each and every keystroke you make, save the information to a hidden file, and automatically upload it to the hacker's computer.

What else can a Hacker do?

There are a number of reasons why a hacker would want to break into your computer. He may use your computer and ISP account for illegal activity, like distributing child pornography. One of the most recent uses of Trojans is to cause DDoS (distributive denial of service) attacks. In a DDoS attack, the client commands all of the "servers" located on individual PCs to attack a single website. Thousands of individual PCs can be commanded to access a website like eBay or Yahoo at the same time, clogging the site's bandwidth and causing an interruption of service.

What can I do to Protect my Computer?

- Only download or accept files from reliable sources.
- Use a firewall to block unauthorized access to your computer.
- Install a good virus scanner program and update virus information files often.
- Do not keep passwords, bank or financial account numbers, social security numbers or other personal and confidential information on your computer's hard drive.

Crime in the computer generated superhighway is the new phenomenon in contemporary scenario. There is no business without E-Business and E-Commerce in our dynamic society. In our daily life we cannot think of any intellectual and necessary work without Information Technology. But this new multimedia technology is being misused and abused by deviants and criminals. Therefore, we cannot think of crime or criminals apart from Cyber Crimes or cyber criminals. Cyber Crimes cause more harm to society than traditional crimes. Hacking attack on Bhabha Atomic Energy Centre, AIMS, World Trade Centre etc are examples of cyber hacking causing more harm to human life than traditional crimes. Whether hacking, spamming, cyber theft, cyber fraud, cyber terrorism, unauthorized access to computer and computer system etc are to be recognized as more grievous than any ordinary crimes. This is a burning question world-wide.

Therefore, to secure our daily life, business and every intellectual conduct, we have to think of prevention and control of Cyber Crimes and specially the most dangerous one that is cyber hacking. It is very complex phenomenon because cyber world does not have any specific territory or jurisdiction as such.

Hacking in cyberspace is not only national but also international legal challenge which requires global standard security measures and controlling policy through worldwide intensive study and research.

People generally understand Cyber Crime as hackers and hacking. Films, TV, new multimedia technology encouraged people to identify the advantages as well as the risks and dangers of new technology in the era of convergence. Therefore, we have to undertake intensive study to know about the relationship between new media, technology and hacking in cyber world and to evolve effective, preventive, as well as controlling measures. Traditional laws and orders become inadequate in cyber world even the Information Technology Act 2000 is also not adequate to some extent in contemporary dynamic era of communication convergence and new multimedia technology.

Hackers usually represent themselves as

i. The protector of vulnerable and insecure information;

ii. Their activities are within legal boundaries; and

iii. That they are not always law-breakers.

This may be because they are confident that

a. Very few or only a few victims are interested to lodge complaint against them.

b. Most of the times victims are unable to identify them. This is due to unspecified and undefined jurisdiction in cyber world. The accused generally commit crime thousands and thousands of miles away.

c. Again another advantage for hackers for which they repeat crime commission is that it is very much complex to understand crime in cyberspace. For example, hackers view one webpage and by deep linking get information which are very confidential without the consent of owner and download it intentionally and dishonestly; it is a complete case of theft under s. 378 of the Indian Penal Code that if any person with dishonest intention takes away any moveable property from one place to another place without the consent of owner or possessor, it is theft.

d. It is also very difficult to identify and understand the unauthorized use which is criminal trespass under s. 441 of the Indian Penal Code, as well as hackers who cause damage, after data or change data etc Therefore, expert hackers think that cyberspace is their exclusive zone and they can do anything whatever they wish very tactfully. They not only cause harm to technological and economic dominion but also to the social, cultural and political values.

This chapter comprising the topics such as hackers, ways of hacking, their culture, international aspect and European Convention, law enforcement in the USA, the UK, and in India to understand what mechanisms are necessary for the prevention and control of hacking in the era of convergence.

In the film 'Hackers', 1995, Richard Gill played by Wendell Pierce, the Chief law enforcement officer says "Hackers penetrate and ravage delicate private and publicly owned computer systems, infecting them with viruses and stealing sensitive materials for their own ends. These people ... are terrorists". This movie deals with the hyperbole with which hackers are represented and the shallowness with which hackers are understood. He had suggested that hackers are like as rapists.

In United States v Edward Cummings — It was held that mere possession of technology which is unauthorized use is a crime. In this case Ed. Cummings was identified as a "danger to the community" for being in possession of a "red box" which is a small modified Radio shack speed dialler. The device was altered to emit-one to make telephone calls free of cost from public pay phones. This was unauthorized use of telecommunication service and he was charged for the same. Another event also proved that the accused had custody and control of hardware and software i.e., an IBM "think pad" laptop computer and computer disks, was used for altering and modifying telecommunications instruments to obtain unauthorized access to telecommunications service.

R. V Gold in the UK, Mr. Verma IIT, Kharagpur hacking of ex-employer's source code and thereafter was arrested by Central Bureau of Investigations in India with the help of Federal Bureau of Investigations in the USA, Ankit Fadia's Denial of Service Attack case in India etc are example that hacking causes threat to social mechanism and pause social progress which is a global legal challenge and there is an urgent need to prevent and control hacking world-wide.

1.2 Nature and Character of Hackers:

According to Helen Nissenbaum hackers never were part of the mainstream, but their current reputation as villains of cyberspace is a far cry from the early days when first and foremost, they were seen. Many say that with their deviant behaviour, hackers also serve to remind the technological vulnerability and ignorance in our society along with law enforcement officials and legislators. The ever growing cost for hacking are justified since the evil actions of computer hackers as also phreakers, crackers, carders, computer pirates and so forth have evidently proved that they might be really harmful and if successful, cause even more tiresome and unexpected costs. In 1960s hacking started with Telephone systems and services as phreaking and immediately spread to computers, computer system, and network.

According to Webster's Dictionary hacker means "a computer enthusiast who is especially proficient or a computer user who attempts to gain unauthorized access to computer systems." Webster's II New Riverside University Dictionary defines hacker as "one who gains unauthorized usually non-fraudulent access (use) and those who enjoy investigating computer operating systems." Bruce Sterling, the author of the Hacker Crackdown, observed that the term hack 'can signify the freewheeling intellectual exploration of the highest and deepest potential of computer systems. Hacking can be described as the determination to make use of computers and information as free and open as possible; and can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit'.

The new Hackers Dictionary written by Hackers offer six definitions for hacking and hackers. Those are as follows:

- A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to many users, who prefer to learn only the minimum and necessary.
- One who programs enthusiastically (even obsessively).
- A person good at programming quickly.
- An expert in a particular language or operating system, i.e., a UNIX hacker.
- One who enjoys the intellectual challenge of overcoming or circumventing limitations.
- A malicious meddler who tries to discover sensitive information poking around.

It also presents two basic principles hackers live by

i. The belief that information sharing is a powerful positive good and that it is an ethical duty of hackers to share their expertise by writing free software and facilitating access to information and to computing resources wherever possible;

ii. The belief that system cracking for fun and exploitation is ethically all right as long as the cracker commits no theft, vandalism or breach of confidentiality.

In Information Technology, a 'hack' is a quick fix or clever solution to a restriction. Tricking a dumb machine into performing an unintended task was the predominant characteristic of a hack. Even a simple trick like sticking cell phone or re-use of pre-recorded tapes as 'blank' tapes can be described as a hack. Experts may know how to cause unauthorized access of program in a computer but does not do so. But a malicious hacker executes programs in others computer programs without express or implied permission of the authority.

Malicious hackers thus engage in criminal activities. Computer users are forced to spend huge amounts of money on specialised programrs, technical staffs, devices etc to safeguard their property. Otherwise only good password entry control, a number of trespassing warnings, screen banner like door and lock system would be sufficient to meet a standard of due care and caution.

1.3 Culture of Hackers:

Individually, many hackers are antisocial. Their intense interest in computers and programming can become a communication barrier. Left to his or her own devices, a hacker can spend hours working on a computer program while neglecting everything else.

Computer networks gave hackers a way to associate with other people with their same interests. Before the Internet became easily accessible, hackers would set up and visit bulletin board systems (BBS). A hacker could host on his or her computer and let people dial into the system to send messages, share information, play games and download programs. As hackers found one another, information exchanges increased dramatically.

Some hackers posted their accomplishments on a BBS, boasting about infiltrating secure systems. Often they would upload a document from their victims' databases to prove their claims. By the early 1990s, law enforcement officials considered hackers an enormous security threat. There are many websites dedicated to hacking. The hacker journal "2600: The Hacker Quarterly" has its own site, complete with a live broadcast section dedicated to hacker topics. The print version is still available on news stands. Web sites like Hacker.org promote learning and include puzzles and competitions for hackers to test their skills.

Not all hackers try to explore forbidden computer systems. Some use their talents and knowledge to create better software and security measures. In fact, many hackers who once used their skills to break into systems now put that knowledge and ingenuity to use by creating more comprehensive security measures. In a way, the Internet is a battleground between different kinds of hackers — the bad guys, or black hats, who try to infiltrate systems or spread viruses, and the good guys, or white hats, who bolster security systems and develop powerful virus protection software.

Several criminologists have attempted to understand and examine the reasons of hacking or why hackers indulge in delinquent behaviour. Hackers are becoming so uncontrollable that it has become very difficult to cope up with the situation worldwide. Hackers originally were computer professionals who adopted the word hack as a synonym for computer work executed with a certain level of craftsmanship. Thereafter they gradually became desperate to spread usefulness and accessibility of computer and computer system among general people.

But nowadays hacker and hacking have changed their meaning dramatically. To hack means to break into or sabotage a computer system and a 'hacker' is the perpetrator of such activities. Legal meaning of hacking is associated with the act of obtaining unauthorized access to program or data held on a computer system or alter, modify or delete etc, any computer program or attempt to do so.

The term Hacker is used to describe any one of the following:

i. **HACKERS.** They knew computers in and out. They can make the computer do nearly everything they want it to do.

ii. **CRACKERS.** They break into computer systems and security thereof.

iii. **CYBERPUNKS.** They are the masters of cryptography.

iv. **PHREAKERS.** They combine their in depth knowledge of the Internet and the mass Telecommunication system.

According to SRI International, who studied more than 80 hackers and their associates in the year 1996 in the United States of America and Europe, 'the concept of honourable pursuit of hacking earlier had largely disappeared'.

In contemporary phenomenon, malicious hackers regularly engage in fabrications, exaggerations, thievery and fantasy. They represent themselves as too idealistic and champion in cyberspace. And that 'Little guys' working against big computer vendors and doing good in long way, juvenile hackers represent themselves as superman of cyberspace.

Hackers presume that general people are having an immature and excessively idealistic attitude towards hacking in cyberspace. Hackers require the knowledge about the technological and operational aspects of the system they attack. Intelligent talented individuals who obtain responsible positions in Information Technology are more technically involved in hackers group. Most hackers are well aware about their illegal conduct and consequences. And at the same time they are also aware about vulnerability of law enforcement agencies i.e. Police, Federal Bureau of Investigation (FBI), secret service etc

At this juncture it may not be impertinent to refer to one case called 'master spy' in the year 1994 which posed a major threat to the US security system. The military chiefs feared that an East European spy ring had successfully hacked into American Air Defence Systems and thereby learned some of its most confidential intelligence secrets. After 13 months due inquiry and investigations it was found out that a 16 years old British music student was responsible for these break-ins. The accused, known as Data Stream 'Cowboy' had downloaded dozens of military files including details of their research, development and other confidential informations. He had also used a company's network of California for more than 200 logged security breaches by using 1,200 computers and modem. He was tried and convicted in 1997 and was fined $1,915 by a London court. After his conviction, the media offered the musical hacker considerable sum for writing book and film of his own story. But he declined and preferred to continue his musical studies and concentrate on winning a place in a leading London Orchestra.

1.4 Types of Hacking:

i. There are various possible ways of hacking of which one is for the malicious hacker to physically enter into the premises of others containing the computer and impersonate its owner. That is like criminal trespass under 441 of the Indian Penal Code. Such impersonation is very easy if the owner has no protective and security system with secret password to start or initiate operating system.

ii. Even the intelligent hacker may be able to guess password where it is required by using password cracking tool. Password cracking tool tests many passwords, find it if written somewhere else, observe it during use i.e., shoulder surf.

iii. If this fails and the hacker cannot start the computer without a proper or correct password then the hacker can reinstall the operating system. This process of hacking is little more difficult and time consuming, but not impossible.

iv. Another way to gain control is for the malicious hacker to deceive the legitimate user into entering and executing a Trojan horse program in the computer. A Trojan horse program contains computer instructions unknown to the user and it perform the hacker's attack.

v. Again the hacker may take advantage of a known vulnerability of a computer operating system such as UNIX or Microsoft Windows which is most technical method and requires detail knowledge of the operating system unless a pre-packaged search tool such as SATAN.

vi. Password is not only a contributory factor for hacking but also an unauthorized access tool. Password may be called as unauthorized access device; though its main function is to identify person or relate with individuals by giving them identity in cyber world. Password contains secret, personal information's or personal identity. Nowadays we have password for everything e.g. for e-mail, ATM machines, Websites, administrators, credit cards, online banking, brokerage, web auctions, microwaves, cable boxes, garage, door openers, bags etc Password crackers are highly sophisticated and keep trying words, letters, and symbols combinations until it hits the right one. Sometimes they have knowledge about that person and about his or her personal particulars whose password they are going to crack and use those particulars till it hits the right answer to open.

vii. Use of mathematical algorithms in an attempt to break the password hash or cryptographic scheme is another way of cracking as well as to protect the password itself. Most of the hacker sites therefore, contain large numbers of password cracking programs e.g., UNIX, Win_9X, Zip files, chat software, e-mail software.

viii. Most of the times hackers target servers because vital information's are stored rather than their client's machines.

A Hacker *prima facie* tries to operate the internet and the telephone networks. Hackers also use scanning process to scan hosts internet activities for remote vulnerabilities through quick fiber-optic connection. Malicious hackers actually focus to attack and crack the installed firewall of a network. Therefore, whether password or PIN number or Social Security Number (SSN) every such number must be kept in head and not in writing anywhere. Again when one has only one password then it is not difficult to remember but if one has three, four, five or more passwords then it is very difficult to remember and have to be written somewhere and any one can access it if not kept secretly. To prevent password cracking is the first and foremost duty, with other duties is to change it time to time, because it is the key to open the security system and confidential information's.

ix. Hacking may be done by sending messages through e-mail, websites, mobile with several offers and pornographic accesses and asking their password or social security numbers and personal information's.

x. Jim Falls Worth worked mutually with hackers to understand the goals of the penetration testing as others call it as friendly hacking. And he comes out with some steps and procedures which criminal hackers use without owner's permission. These are as follows:

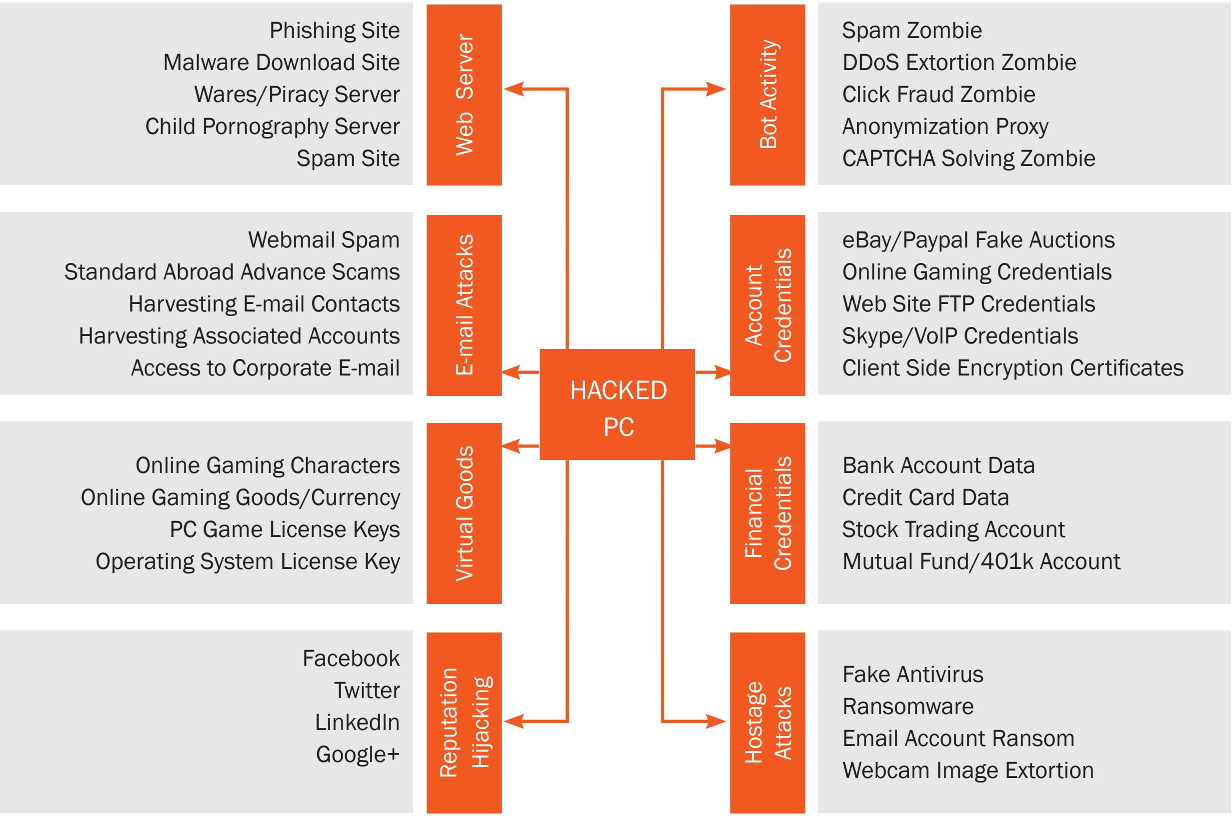


Fig. 1. Possible ways of Cyber Hacking

(1) They assess the strength and weaknesses of banks' new services and how they relate to the rest of the bank's operations. (2) They try to determine what vulnerabilities exist within those systems. (3) They offer solutions to increase the security of the systems. (4) They demonstrate the possibility of losses to bank or its clients by breaking into the bank.

The kinds of information upon which hackers are interested are as follows:

1. Operating systems.
2. Open technique and systems in use.
3. Major vendors used within the enterprise.

4. Physical address of data centre and telephone centres.

5. Phone exchanges information etc

6. Another way of attack is denial of service attack as developed in recent past.

7. Hackers may hack for evidence, when they find out that their activities are under investigation and then they try to delete investigators file.

Hackers and their culture both are very much technological. Their language is based on jargon which is the point of separation from mainstream. It is very difficult to identify an obvious structured group who are acting on a computer underground. New generations of young people are growing up every moment with computers.

1.5 What is Hackers Group?

The word "hack" began as a term for an "ingenious solution to a problem." Then, with the onset of computer programming, it evolved to mean "a feat of programming prowess." Teenage boys, attracted to the elite power they could wield, immersed themselves in a world of Internet bulletin boards and telephone systems. The lure of the next big challenge, hacker-group rivalries, political activism and personal gain all come into play in this fascinating underground world — in which everything is painted in shades of gray.

Hackers, virus writers, unauthorized users in cyberspace have no organization as traditional criminal group. Hackers generally change their password, methods, sites, group membership and e-mail address. Therefore, it is a very difficult task to track hackers and their group. Teenagers to older people, poor to rich people again school going children to engineers and men as well as women are involved in hacking and other Cyber Crimes. This is major threat and shock in the cyberspace. These are increasing with development of technology in the era of convergence.

1.6 Changing Nature of Hackers' Culture:

Hackers on both sides overwhelmingly support open source software, programs in which the source code is available for anyone to study, copy, distribute and modify. With open source software, hackers can learn from other hackers' experiences and help make programs work better than they did before. Programs might range from simple applications to complex operating systems like Linux.

There are several annual hacker events, most of which promote responsible behaviour. A yearly convention in Las Vegas called DEFCON sees thousands of attendees gather to exchange programs, compete in contests, participate in panel discussions about hacking and computer development and generally promote the pursuit of satisfying curiosity. A similar event called the Chaos Communication Camp combines low-tech living arrangements — most attendees stay in tents — and high-tech conversation and activities.

Hackers are not always malicious rather they are ethical. They are also not always interested in purely academic endeavours. All the hackers in the contemporary phenomenon are not expert on computer science or engineers of computer programming. 1st generation hackers were computer science experts or engineers who wanted to act for public interest. 2nd

*"It is compassion, the most gracious of virtues, Which moves the world."- **Thiruvalluvar***

generation hackers mostly dealt with telephone services, tampering source code to cause injury to computer, computer system and network. 3rd generation hackers were mostly young people who committed hacking as fun, game, entertainment, revenge and to make money quickly. 4th generation is the contemporary scenario where hackers are crackers, denial of service attackers, person who clone telephone and internet connections, cyber- terrorists and spammers. They are elderly, young, female, male, educated, non-educated etc From 1st to 4th generation hackers activities are different; they are members of heterogeneous group.

That is why nowadays police personnel trainings are very essential. Five police personnel of the Cyber Crime Cell were undergoing an intensive four month internet training in 2001 in India. Within this four month they became as good as hackers and better equipped to handle Cyber Crime with new techniques of hacking on the internet etc This is very urgent need of our society because to prevent and control hacking, policemen have to know how crimes are committed in the superhighway.

On 10th July, 2001, trainer Mufti said *"the policemen's favourite topic is writing of business applications or the internals of the Net. They are also concentrating on Java and C++ languages and are surely becoming more confident each day"*. One police inspector Zahid said *"we are glad to undertake this intensive four months course. Whatever is required to know for policemen to combat Cyber Crime is being taught"*. So, the hackers cannot escape the Law for long. Mumbai Police Cyber Crime Cell has its website, www.CyberCrimeCellmumbaicity.com. They organised several seminars and workshops on Cyber Crime, hacking, internet misuse and like.

On 20th January 2005, News line published in website that in England and Wales police officers, who has little or no training, are required to receive basic training in tackling Cyber Crimes. This training course may be called as 'net crime training and delivery' program. Because if they do not know what is in front of them, how they can seize it! Computer crime is now very much part of the main stream policing and any crime has an otherwise Information Technology component in contemporary Hi-tech society.

1.7 Cracking, Phreaking and Hacking:

Malicious hackers, who usually "crack" down network security, secretly enter into security system to cause international damage, which are also called as "Electronic Vandals", who can break security system whether it is of Government department or private industry or individuals. Not only that, hackers are most of the times intellectual programers who has special study and knowledge about computer system and they use their skills to cause trouble, steal credit card numbers, flow viruses etc of those hackers who are involved in illegal programming act to break into others computer system, and network security are called crackers.

Therefore, we can say when hackers cause grievous or dangerous harm to computer and computer system or network security system and break systems they are called crackers. They not only commit criminal trespass or unauthorized access but also commit other crimes. Crackers usually try to attack server where they will easily find vital information of numerous users. Therefore they target through internet and telephone network. To achieve success in cracking or malicious hacking, they eventually use scan program to scan hosts. Phreakers were generally telephone hackers. They illegally enter into computer system through phone.

They illegally enter into computer systems for several purposes e.g. information and sale it out of curiosity or to make fun or game. Phreakers engage in pranks/phreakers by altering phone system, call diverting, rearranging web pages. They do so sometimes without any aim to gain financially though their activities cause loss to corporate bodies, Industries, Government Departments Individuals and so forth.

As hackers do phreak out of curiosity as well as to gain such reputation he or she is the excellent personality who has intelligence and knowledge in new multimedia Technology. They find bugs or holes in computer systems and network through which they can enter into and exploit by alteration, addition, damaging or destroying any data or device in computer or computer system or network as such. Hackers or phreakers who flow viruses or shut down internet websites and make any error for internet service providers are also called as "denial of service" attackers, spammers.

We can say, phreakers are forefathers of hacks and hackers. Prior to computer our communications mostly depended on telephone. In public telephone where facilities are available to call by inserting one rupee coin, people do commit such crime. They carefully slide the strip down the slot as far as it may go and pick up the phone and while getting a dial tone they put a coin into the slot and as the phone registered the coin and call is made, immediately they do get back their coin. Thus they make free telephone calls through a piece of stiff construction board which is cut accordingly and is adjusted with slot.

In contemporary phenomenon through computer, one can communicate with mobile phone, wireless and land phone which makes phreaking or telephone hacking become easier.

1.8 Behaviour of Hackers':

Most of the intensive study of criminologists in the contemporary hi-tech society is based on hackers and hacking. Several criminologists have attempted to understand hackers' behaviour and to examine the causes for which hackers are involved in delinquent behaviours and to develop effective legal principles for the prevention and control of this dangerous crime although we know complete elimination of Cyber Crimes is not possible in the cyberspace.

Some jurists say that hackers commit crime due to passion or tendency or addiction to use computer and to act with network e.g., hacker Bedworth in 1993 was arrested in England and his advocate took defence that he was suffering from a psychological addiction and irresistible impulse to use computers, computer systems and network on which ground he was acquitted.

It shows that hackers in the new generation do not require intensive study and in-depth knowledge about computer science or programming aptitude; they are not always computer or information technology engineers. Therefore, today's hackers are different from what they were earlier. New generation hackers are involved in delinquent activities as a fun game or sport and they are not even interested to develop their knowledge on new multimedia technology academically. They are more interested to take revenge or to fulfil their greed or to show their power or to do other malicious act through computer system and network.

Prevention and control of hacker's activities become more and more complex from time to time because they are the members of heterogeneous group and not of homogeneous group. They do not have any generic fabric. Some hackers are called as sport intruders who break in computer system, internet and deface web pages; and others are competitive espionage who generally avoid illegal activities and act in ethical manner. They are also group of intelligent youth who do hack to save their nation and to keep security in their country with authority.

Hackers are most of the times male teenagers, who are and were neglected children at their early age, habitually, addicted for drugs and alcohol they are generally very smart but with poor educational performance, they are pleasant and representable personalities with patience to sit well at the keyboard and monitor hours after hours. The new multimedia technology is changing every moment. Therefore what was in 1970s has been changed in this new era of technological millennium. So with the change of society and situations, hacking culture is also changing time to time. Even though we can classify them like hackers, crackers, phreakers etc, but dividing line is very thin and overlapping.

1.9 International Initiatives to Prevent and Control Cyber Hacking:

1.9.1 The European Union:

To discuss any one of the Cyber Crimes we must refer to the European Committee (EC) on Cyber Crime Problems. This committee formulated a committee of experts on crimes in cyberspace and they made a draft Convention on Cyber Crimes, Draft No. 25 REV. 5, on December 2000, which was followed by the Cyber Crimes Treaty on 23rd November 2001. This was the first International Treaty with about 45 signatories to specifically target the Cyber Crimes.

There were 3 main parts to the convention: First part contains common definitions of certain offences relating to the use of new technologies, i.e., s. 1 of Chapter II Substantive Criminal Law. This section consist of 4 main offences i.e., Title 1 which deals with offences such as hacking, virus attack, denial of service attack e.g. Art. 2 prohibits illegal or unauthorized access; Art. 3 prohibits illegal interception; Art. 4 prohibits data interference; Art. 5 prohibits system interference, Art. 6 prohibits misuse of devices.

1.9.2 The Global Internet Liberty Campaign (GILC):

It brings draft proposals to empower the law enforcers to intercept international communications and traffic data with the hope to give police forces free range to wire tap or to access internet users to prevent and control abuse. Though, Walter Schwimmer (Secretary of EC) objects that this proposal allows the free hand for investigations without first establishing the controlling measures to check if they have done something wrong. This measure is open to abuse by law enforcement bodies. One proposal of the treaty was to outlaw "hacking tools" with internet security tools. Again GILC members say that this would impose unnecessary restriction on the legitimate promotion of computer security technologies. Some suspect that the treaty may go contrary to the protection of human rights and also it may undermine the development of network security techniques as well as it may reduce accountability of government in law enforcement.

The Council of Europe has developed the measures on Cyber Crimes to cop-up with the international growing threat in cyberspace. This is not only to tackle the criminals who are using the internet to carry out financial theft and fraud but also to tackle Denial of Service attacks and computer viruses, cracking etc which are potentially very damaging in nature.

The Group of Eight (G8) made up of the world's most wealthy Industrialised nations, met on 24th October 1997 to discuss the issues and take a lead from the council of Europe in drawing up a global treaty. Yaman Akdeniz, Director of Cyber Rights and Cyber Liberties, which is part of GILC, argues that the council of Europe's treaty would deny European internet users the right to be presumed innocent until proven guilty.

The challenges that law enforcement agencies face in our battle with Cyber Crimes are generally being divided into three categories. These are as follows:

i. Technical that hinders law enforcement ability to find and prosecute criminals operating online.

ii. Legal resulting from laws and legal tools needed to investigate Cyber Crime lagging behind technological, structural and social changes.

iii. Operational to ensure that we have created a network of well-trained, well-equipped investigators and prosecutors who work together with unprecedented speed even across the national borders.

When a hacker disrupts air traffic control at a local airport or when a cyber stalker sends a threatening e-mail to a school or a local church or when credit card numbers are stolen from a company, then investigators must locate the source of communication e.g. find the electronic criminals who are responsible for E-threat or E-robbery and other E-crimes. James K. Robinson said that to accomplish this, law enforcement agencies must in almost all cases trace the 'electronic trail' leading from the victim back to the perpetrator tracing a criminal in the electronic age.

However, it can be difficult especially if we require international co-operation, if the perpetrator attempts to hide his identity, or if technology otherwise hinders our investigation. In the contemporary phenomenon of liberalization and globalization, E-commerce and E-communication are expanding worldwide by making consumers and business concern more vulnerable. The global nature of the Internet is the contributory factor for hiding identity and Cyber Crime internationally. For example, a computer hacker in the UK might attack the computers of a corporation located only a few miles away or in India, France and the USA. The situation is very complex for the law enforcing agencies to investigate and arrest criminals who wave communication through multiple countries. What is most important is the international co-operation and assistance; without this, deviants will commit crimes freely again and again only with the help of a computer and modem or only with internet connecting devices.

In February 2000, the Denial of Service (DOS) attack is good example of how easily crimes can be committed in superhighway and how much the international co-operation is necessary for technical and infrastructure challenges. To tackle the global communication, every country has to work across the borders very quickly before information is altered or deleted or misused by hackers.

It is very necessary to deal with hacking in global scenario. Therefore, here we will deal with prevention and control of hacking in the UK, the USA and Indian scenario.

1.10 Cyber Hacking in the United Kingdom:

While explaining situation of hacking in the United Kingdom (UK), Professor L. Lloyd says, "the stereotypical depiction of a cyber hacker tends to be that of a male teenager in a greasy T-shirt and torn jeans who spends hours slumped over a terminal, eyes gazing fixedly at the green glow of the VDU monitor ... Nowhere is safe, no one can keep him out, no one knows of the scale of the threat, the silent deadly menace stalks the networks as seen in R v Gold".

1.10.1 Audit Commission:

On the basis of prevention is better than cure the UK Audit Commission recommended some preventive measures with the British standard for information security management. The reports identified certain security polices which are very urgent to follow:

- Cyber security which is adequate with business strategy.
- Clear statement of the importance of cyber security.
- Clear statement of the adequate and proper law regarding Information Technology security.
- Clear statement of the responsibilities of staff to protect investment in new Technology and computer data.
- Clear statement of the steps taken by the management to encourage to adopt and maintain high security standards as well as to enforce it in reality by the management.
- Statement of the steps taken to reduce computer misuse i.e., secure password systems etc
- Statement of data processing through new hardware and software.
- Internal control mechanisms. These all are with the tune of the British Standard for Information Security Management (BS 7799) such as key controls, security document, education and training, responsibilities, reporting, virus controls, data protection etc

1.11 Cyber Hacking in India:

In the globalised, liberalised era of communication convergence and new technology, the server is in one State and user in other State. The application of law in cyberspace is very complex due to undefined jurisdiction. It is international as well as national legal challenge. India enacted and passed the Information Technology Act 2000 (Information Technology Act) as implemented on 17th October 2000 and Rules 2000 following the United Nations' Model Law, 1997. The Information Technology Act 2000 specifically ss. 43 and 66 deal with hacking and unauthorized access to computer, computer system and computer network. In the strict sense these are not related to other medias with internet or network connections e.g. Wireless, Mobile, Television etc But if we interpret these in the liberal sense then we can see other Medias with internet or network connections e.g. Wireless, Mobile, Television etc are also included under these two sections.

The term hacking is synonymous with unauthorized access and criminal trespass. Hacking is associated with the act of obtaining unauthorized access to program or data held on a computer, computer system, computer network or alternative, modification, deletion, destroy of any computer program or attempt to do such unauthorized access. In the USA and the UK hacking is understood as unauthorized access and prohibited under the Computer Fraud and Abuse Act 1986 in the USA and the Computer Misuse Act 1990 in the UK.

Therefore, we can say, hacking is a prohibited conduct which is prohibited by State through criminal law that is, the Information Technology Act and the Indian Penal Code in India, and State prescribes punishment for hacking through criminal law. Cyber hacking is related to computer, computer system, computer data, computer program. Therefore, we must know what is 'computer' in the era of communication convergence.

1.11.1 Essential Elements of Hacking:

Essential elements of hacking are as follows:

❖ Causing intentional wrong or damage to other.

❖ Causing wrong or damage to other with knowledge.

❖ It must relate to computer, computer system or computer network.

❖ The result must be to (a) destroy, (b) delete, (c) alter, (d) diminish the value or utility of information, or (e) affect injuriously.

In contemporary phenomenon urgent need is to adopt uniform and high standard cyber laws and specially law on Cyber Crimes to adopt more teeth to combat the situation. India and Pakistan controversies on Cyber Crimes are in a rising mode. Industries are ignorant about even inside cyber hackers. People are addicted to pay for e-business; most of the sites do not have up to 75 bits encryption techniques which is minimum requirement to prevent threats in the cyberspace. Credit card hacking is increasing day by day. Websites for example, rediff.com, Yahoo.com, satyamonline.com etc simply asks for credit card numbers with other details for e-shopping and e-commerce. And their responsibilities are up to payment and not till the delivery of the goods to the consumers; these processes are exploited by hackers. These caused two way hacking:

1. If user is actual card holder and given original information then hackers easily use it to commit other crimes i.e. identity theft, cyber fraud, sell it to others etc

2. If user is not actual card holder and giving wrong information about credit-debit card, then the companies and other who offer to sale through internet may be in loss.

1.11.2 Socio-Legal Impact of Cyber Hacking in India:

Cyber hacking does not mean no loss to human life because hackers are human being and they are causing injury to human society. Especially Bhabha Atomic Research Centre servers and traffic control servers were hacked; which are direct examples of injury to human life. On 11th

September 2001 and July 2005 recent attack on the USA and the UK are burning, painful and measurable instances in contemporary scenario which made an impact on cyber hacking and cyber terrorism. Those attacks are not confined to those particular countries but also to the world. Therefore, our primary task must be the security measures in cyber world. Pakistani hactivists are successfully defacing several Indian websites from 1999. Now-a-days it has become common practice between hacker groups.

In 10th January 2001, R.K. Ragavan said it is very difficult to nail on Pakistani hackers because the Indian hackers are not conniving with the Pakistani law enforcers. Therefore any prudent person can think about the kind of co-operation India may get from Pakistan. Hackers generally break-in and steal information from computer system by using softwares. Those hackers have thorough knowledge of that software. In the year 2000 about 635 Indian websites were hacked. It was very complex phenomenon to even identify hackers. People of India are most of the times illiterate and reluctant about this crime and complaint. Mr. Dewang Mehta, President of NASSCOM says that the lack of uniform laws against Cyber Crimes involving abuse of computer systems made prosecution of cross-border hackers difficult.

CASE STUDY ▶ ***1: IIT Kharagpur, W.B., India (2002) Case:*** Only for co-operation and active collaboration of the Federal Bureau of Investigation (FBI), Central Bureau of Investigation (CBI) in India arrested 27 years old software Engineer, Mr. Shekhar Verma for allegedly trying to illegally sell the 'Source Code' of a sophisticated software package worth about $70 million. The package was called as "Solid Works 2001 Plus". The culprit IIT Kharagpur graduate, was caught red-handed while he was about to sell the same package to two undercover FBI agents at Ashoka Hotel. He believed that undercover FBI agents were the representatives of one US Company. Therefore, he had struck, a $2,00,000 deal with them for the misappropriated source code. He was a former employee of a software company called Geometric Software Solutions Company Ltd. in Mumbai. While he was in service, he took the entire Source Code and after resignation started approaching other software companies in the USA through e-mail which was treated as a very shameful act. This is also to be treated as cyber fraud committed by a hacker.

CASE STUDY ▶ ***2: Hacking in Baroda, Gujarat:*** On 9th June 2005, hackers attacked one website and claimed $10,000 for restoration of website. Indian Police even be came vulnerable. They found no clue to control the incident. Domain name was the issue. The "website" which might had been kept unlocked with registrar was fraudulently transferred and controlled by hackers. Therefore, it is very vital to see the standard of security system of the domain which any one is going to buy from any company or institutions.

CASE STUDY ▶ ***3: Hacker Dr. Neruker:*** On 5th July 2001, the Cyber Crimes Investigation Cell Mumbai received an unknown telephone at about 07:00 PM that their website www.ccicmumbai.com is going to be attacked by hackers. Immediately Police Officers noticed that it has been hacked. They identified the hackers who replaced the original homepage of the Mumbai Police website and posted there obscene comments and abuses to Police Officials. The Police Officers then investigated their server room that is, Net4India and had taken help of the members of Advisory and Technical Committees to analyze the log records. They investigated that Internet Protocol address that was related to this hacking. It belonged to the internet provider company DISHNET SSL LTD, Mumbai and the end user of that same date and time was identified by internet provider immediately. It was a cyber cafe i.e. “Osprey Enterprises” at Dadar, Shivaji Park. Police entered into that cyber cafe and proceeded their search and examination of computers; at last they found out the copy of their homepage in a computer which was replaced and related to software cute FTP. Then Mumbai police seized that computer and took the descriptions of the culprits who used the computers. Immediately the police drew the sketch of the suspected accused. But, other information could not be received from the cyber cafe as they did not maintain it. By repeated visit to Net4India, the police investigated that from the same Internet Protocol address with Internet Service Provider Dishnet there were another two midnight hacking attacks after 30 days of this incident. They, then took the detailed information from Dishnet about the subscribers of the Nexus cyber cafe, Mumbai. During investigation, they interacted with 3 partners of the said cyber cafe.   One of the partners disclosed before the police that one of his partners Mr. Mahesh Mahtre and his friend Mr. Anand Khare had committed the hacking from their cyber cafe. Both the accused were arrested by Mumbai Police Cyber Crime Investigation Cell. Mr. Anand Ashok Khare had assumed the identity as Dr. Neruker and the identity “Da Libran” was assumed by Mr. Mahesh Mhatre. First one is an Engineer in Information Technology fields and the accused is a computer progammer. Though, now so called “Dr. Neruker” is working with Mumbai Police Cyber Crime Investigation Cell for the prevention and control of hacking. In the same way, Mr. Ankit Fadia the famous Indian hacker was turned as security provider.

CASE STUDY ▸ ***4: Delhi Hackers’ Case:*** Delhi Police arrested two hackers on 6th February 2001. It was the most breaking news in India because two people were arrested by the Delhi Police for allegation of hacking a website. This was probably the first case in India where accused were arrested; as said by Police Commissioner Rajan Bhagat. Both the hackers were detained for allegedly blocking the website named goZnextjob.com. This website provides support and information to prospective employers and job-seekers. The accused posted a message on that website declaring that it was closed but actually it was very much open. The hackers were sent to judicial custody for 14 days as they were charged under s. 406 of Indian Penal Code 1860 i.e. criminal breach of trust, and s. 66 of the Information Technology Act 2000 i.e. offence of hacking. Though they were denied bail by the Metropolitan Magistrate on 8th February 2001 after they were arrested on 6th February 2001; on 12th February 2001 Additional Sessions Judge of Delhi, Mr. P.K Gauba granted bail to those two hackers who were the partners of software solutions Mr. Amit Pasani and Mr. Kapil Juneja.

In December 2001 Indian websites of AIIMS, the Atomic Energy Research Board, Delhi High Court Bar Association etc were hacked eventually. Victims were busy developing their internal system, anti-virus software and firewalls rather than reporting the police. Perhaps they wanted to avoid negative publicity and they thought that it may deter their potential customers. Government was under false sense of security about companies, netizens and websites. This is the scenario worldwide. However, at the same time, detections, investigations, convictions for

Cyber Crimes systems are in existence and functioning worldwide. In India, Police personnel are undergoing intensive training about prevention and control of hacking and other Cyber Crimes. India has constituted several Cyber Crimes Investigation Cells to the same end.

CASE STUDY *5: Hackers "Phishing":* Worldwide hackers are pursuing the method of 'Phishing' to drive spam, Junk mail, advertisements and several offers. Bangalore Police detected only between July and December 2004 about 10,310 phishing attack by hackers. Hackers most of the times preferred to use financial service sites, healthcare sites, online etc to make netizens vulnerable. Symantic blocking was over 33 million a week between July to December 2004. Though, in the beginning it was a million a week. Hackers are using spam in contemporary scenario to steal confidential information such as identities, passwords and accounts.

CASE STUDY ***6: Hacking Between India and PakistaN:*** Hacking took new shape between India and Pakistan that is, net-war by way of defacement and control of websites of each other. In the year 2005, almost 114 Pakistani sites have been hacked by Indian hackers and about 766 Indian sites were hacked by Pakistani hackers. In the year 2004 almost 288 Indian sites were hacked by Pakistan based hackers.

According to Mr. Anubhab Kalia, "for every Pakistani site defaced by Indian hackers, the Pakistanis hacked into 10 Indian sites. There is a constant game of gunmanship happening online". One analyst of Pakistani system said "a good number of websites have been set up by Indians in a web of deceit, with the main aim being to lay the blame on Kashmiris and Muslim". I will discuss this point in detail while I will discuss Cyber Terrorism in the subsequent chapter.

CASE STUDY ***7: Arrest of the Two Indian Computer Trainers at Chhattisgarh in 2001:*** One Manoj Singhania head of the local branch of Aptech and another Prakash Yadav, in charge of training institute were arrested for allegedly sending e-mails in the name of Microsoft and Videsh Sancher Nigam Ltd. (VSNL) India. The e-mails contained program file named 'Speed. exe.' The moment the exe was opened, it would automatically send the password, data and other information of the user or users to the accused. They had also tried to hack into the computers of the State Bank of India in the same way.

CASE STUDY ***8: Arrest of Ex-Scientist in the Year 2001:*** Even on 21st September 2001, one ex-Scientist was arrested from ISRO for E-mail threats to the Department of Atomic Energy and hacking of an Internet Service Provider, Icenet at Ahmedabad; India and also for sending e-mails treat to the nations security which is also to be treated as cyber terrorism.

CASE STUDY ***9: ATM Hacking:*** The complaint was filed by one private firm that the money had been withdrawn on 30th July by using a password which was hacked by accused. On Tuesday, 10th August, 2004, the New Delhi Police arrested 27 years old hacker Mr. Rajesh Malhotra. He was charged for hacking an ATM machine in Mayur Vihar and for withdrawing Rs. 3 lakhs. Police also seized from the accused the same amount. But he was released on bail thereafter.

CASE STUDY ***10: Mobile Phone Hacking:*** In the year 2006 most of the hackers had started to misuse of mobile phone, hacking its software and cyber spying through

The manuscript looks chaotic, even by mathematics standards. An equation means nothing to me unless it expresses a thought of God. ***- Srinivasa Ramanujan Iyengar*** contemporary communication convergence technology and mobile commerce. No doubt, world is moving very fast and complexities are also. To fill in gaps, the Government law enforcing agencies and Non-Government Organizations are very keen to develop new measures. As ethical hackers i.e. Ankit Fadia, Dr. Neruker, Neeraj etc are employed by Government and are evolving new software to prevent and control cyber hacking but at the same time malicious hackers are accessing those software through World Wide Web and playing their role to commit crimes with new dimensions.

In the August 2007, hackers developed Trojan horse a type of virus and programd it to send out personalised e-mails to Monster.com users known as job opportunity site and the program asked user to submit bank details. Through this program about 1.6 million entries such as names, detail identity, addresses, telephone numbers and so forth were stolen by hackers. Hackers used the identical way of phishing where users are very often asked to enter personal details. This year the spammers celebrated Valentine's Day as Cheers day. In 13th February 2008 Neeraj Kaushik, country manager TrendMicro says, “Nearly 2.15% of spam originates from India. The top 20 spam producers will always have one or two Indian service providers in the list. For example Bharati and BSNL were in the list this month.” He also said that about 15% of spams carry some virus e.g., Trojan horse. The West Bengal National University of Judicial Sciences, Kolkata was forced to remove its website www.nujs.edu on 5th February, 2008 as hackers linked it to a pornographic site which caused embarrassment to all visited dignitaries. However the University suspects it has not been done by any students rather by visitors, who logged to get information about the Law School’s Cultural Fest from 7th to 9th February, 2008.

CASE STUDY **11: *Mr. Bharadwaj Case.*** In the year 2001, Mr. Bharadwaj, Managing Director of IGSP Technology Centre India Pvt. Ltd. filed an FIR at Chandigarh about hacking of ‘computer system’ under ss. 66(1) and 66(2) of the Information Technology Act 2000 and s. 380 of the Indian Penal Code 1860 before police. That, Techno Noble Info Way Ltd. (TNIL) had illegally downloaded some data from their server in the US The Police officers started immediate search of TNIL office premises and confiscated the server, related devices used in the crime. Though, accused’s plea on the other hand was that IGSP committed breach of contract due to not providing them minimum service as was agreed.

CASE STUDY ***12: Hacker Kalpesh Sharma’s Case:*** On 26th September 2003, a media news disclosed about hacker Kalpesh Sharma as he was put behind the bars in Ahmedabad. He was arrested on 24th September by the Cyber Crime Branch of Mumbai Police on a complaint filed by UTI Bank official that the accused hacked the site of UTI, Banks i.e., www.uti.com on July 11 and send an e-mail to the bank authority with a message that “the website is weak and they should provide security”. He expressed that he can do good for security in exchange of Rs. 15 Lakh and posted his contact numbers. Police arrested him from Ahmedabad. He was charged under ss. 66 and 43(b) of the Information Technology Act 2000 and remanded to Police custody till October 6th as Maharashtra Government Counsel stated that the culprit has hacked many other websites and was capable to hack many others.

Case Study ***13: Online Traders Hacked:*** Online trading of shares is not safe as referred in earlier case too. A Ghaziabad based online traders password was stolen by a hacker which was related to shares and caused a loss of about Rs. 5 lakh. The CBI, while investigating the case, referred that in Mumbai, Ujjain and other places in India such types of losses are running into even crore. In the instance case, traders were cheated by hackers. Hackers were getting account information of those traders and using the same they bought shares at very high prices. Whereas, they were then selling it at very low prices which were causing huge financial losses. In the instance case, when one trader was told about the debit of Rs. 5 lakh against his account then he realized about the 'cyber break-in'. However, the trader thought that it might be due to the password problem which they informed to the brokers who were the people to maintain his on line trading account. But, subsequently he realized that that Rs. 5 lakh actually was withdrawn and invested to the account of the accused. He then lodged a complaint to the CBI for cyber hacking, cyber cheating, cyber fraud and registered under s. 419 of the Indian Penal Code 1860 and s. 66 of the Information Technology Act 2000. This is the instance when Pune cyber fraud case and Karan Bahrees case were highlighted and Prime Minister Dr. Manmohan Singh was asking NASSCOM and the Department of Information Technology to come out with new amendments to the Information Technology Act 2000 and to increase punishments for Cyber Crimes.

Case Study ***14: Banks Are Victims:*** One employee of Bank of India tapped organizations computer network, on November 2003. The alleged accused after tapping the computer network gathered data on all keys, passwords, monitoring system and other information. He was arrested by police and released on bail thereafter.

12. Conclusion and Suggestions:

The word "hacker" carries weight. People strongly disagree as to what a hacker is. Hacking may be defined as legal or illegal, ethical or unethical. The media's portrayal of hacking has boosted one version of discourse. The conflict between discourses is important for our understanding of computer hacking subculture. Also, the outcome of the conflict may prove critical in deciding whether or not our society and institutions remain in the control of a small elite or we move towards a radical democracy (a.k.a. socialism). It is my hope that the hackers of the future will move beyond their limitations (through inclusion of women, a deeper politicization, and more concern for recruitment and teaching) and become hactivists. They need to work with non-technologically based and technology-borrowing social movements (like most modern social movements who use technology to do their task more easily) in the struggle for global justice. Otherwise the non-technologically based social movements may face difficulty continuing to resist as their power base is eroded while that of the new techno power elite is growing — and the fictionesque cyberpunk —1984 world may become real.

In this new era of Industrial espionage any one can travel or walk with Pocket PC and login to tap unprotected wireless internet connections in homes or business industries. This is not easily traceable except connection of registered user. As for example, the case of Virginia we can refer here, one morning John Strolls in Virginia was storing logging locations and network address of unprotected wireless internet connections by using the self software and the wireless receivers

Love is over brimming mystery joins death and life. It has filled my cup of pain with joy.
- Sir Rabindranath Tagore

which enable computers to receive wireless signals. While doing so he incidentally identified that an unprotected connection was coming from a nearly located parking garage. Out of curiosity, he immediately passed this information to his partner X (Partner in Crime). After two days when X sat with his laptop computer in the parking garage he hijacks that wireless internet connection which was identified by John. X did so using the basic network information collected during John's survey.

One of the convenient ways of hacking is scanning a network or computer system. By this hackers can control and observe the activities of server. This is in other words called as external attack by mapping through scanners. Because unless one know what is his target he cannot access it . Here we can say, computer systems are becoming more dependent on the network and also becoming more vulnerable. At this point we can refer Wietse Venema and Danfarmer on SATAN release note after which scanning became standard for both attackers and defenders/ victims. Scanning program became very popular which was written by "Fyodor." He encourages people to write to him at fyodor@dhp.com.

Not only the external attack but also the internal attack became very much harmful and therefore, we have to be aware about the technical methods of cracking whether password cracking or network cracking and also controlling measures thereof. Controls may be on application of resources, system or on other infrastructural control. Hackers try to find out whether the system, program or personal data are with weak password, strong password or no password. Whether dialling into modems is with security or without security, whether bypassing the security system is possible or not. They try to find out these information by using their own tools.

Hackers usually try to use social engineering. They also try to learn about the target technology, free tools from the internet and try to build their own tools to gather information. Therefore, we have to have more teeth and nail for preventing and controlling this dynamic and complex scenario. We have to keep in mind that another way to hide e-message is encryption for which always decryption must be available which brings hidden message back to normal text or plain text and then it becomes very difficult to cancel. Therefore, encryption and decryption keys must be used for sending messages and receiving messages both to communicate each other.

On 19th January 1999, Gilmore and Electronic Frontier Foundation announced success. In less than 24 hours they decoded a DES-encrypted message which was their exact goal i.e. Deep Crack. Crypto hacker built a machine at a cost of less than US$250,000 for this attack. The name of the DES-Cracking machine is a take-off on the master-level chess-playing IBM Computer Deep Blue. This is called as Deep Crack ... Everything which was considered as difficult to attack had been cracked by crypto-hackers.

Teenage hackers like Ankit Fadia at 14 years, Neeraj Pattath at 17 years are appointed by the NASSCOM, Mumbai Police and other committees in India to advise (1) to set up anti-hacking measures; (2) to know how to detect hacking; (3) to know how to solve hacking problem. They are to be called as ethical hackers as Kevin Mitnik in USA. A major hack was avoided by Mr. Ankit Fadia when he was only 16 years old e.g. denial of service attack by Pakistani hackers group etc He detected that its origin is in Pakistan.

Even, only by a cell phone a malicious hacker can get control over others cell phone, wireless, computer, websites and sent messages, make call, call diversion, download software, flow viruses, commit cyber terrorism as happened in Ayodhya case in India in the year 2005, commit cyber pornography and other such Cyber Crimes. Therefore, our firewall system must be strong and updated enough to control and prevent hacking. When investigator traced that their files are attacked by malicious hackers then immediately they must shut down the computer after saving all files and disconnect computer from network. For the purpose of evidence, it is very essential to print out what was traced by them.

Every computer user ought to use screen saver and system lock activities. Every prospective user of new multimedia technology ought to get essential training about prevention and control of hacking and how to maintain security system. Another duty is to log on at firewall and internet connection point to prevent hacking attack. There must be clear and uniform law about the Internet Service Providers and cyber cafes responsibility, liability and accountability. They must be prohibited to use the user numbers of their clients as it is very much available to them.

The proposed Information Technology (Amendment) Bill 2006 reduced liabilities of intermediaries, must be implemented. It targeted to reduce punishment for Cyber Crimes, to reduce liability of intermediaries, to change some definition of Cyber Crimes e.g., s. 66 earlier defined hacking and now it is computer related offence, to give executive upper hand over judiciary, to reduce power of police to arrest. Therefore, these particular amended provisions will increase Cyber Crimes and will not be so effective in prevention and control of Cyber Crimes in India.

Though Government and law enforcing organizations are keeping their eyes to combat hacking, this is again true that hacking is increasing day by day in India. That is because of some loopholes in Information Technology law and great illiteracy about the subject amongst the people. Definitely, lack of awareness is vital contributory factor for hacking. Our judiciary also needs some training and infrastructure developments in this field. To achieve the objectives of the cyber law, Indian judiciary may use ethical hackers to find out drawbacks of technology, to help investigation of Cyber Crimes and thereby to assist prevention and control of Cyber Crimes. Laws must be definite on some points e.g., we need to adopt specific and clear definition of Cyber Crimes, hackers, wrongful gain and loss and so forth. Terms like destroy, alteration, deletion, hacker, are needed to be defined in Information Technology Act 2000.

When hackers store information in others computer or in any webpage for example, in own e-mail address with false identity etc, the law is not clear in such a situation and needs to be clarified and settled. Hackers culture, modes of hacking are almost synonymous worldwide whether in Russia, USA, UK, Canada, Australia, India of anywhere in the globe. Again jurisdiction in the cyberspace is multifaceted issue. Therefore, we need to adopt uniform law on jurisdiction issue; it must not be so that only a link is enough to try the case, because there may be link with several countries. In such a situation who will try it? Again for one crime accused cannot be punished twice. Not only that, we need to adopt uniform preventive and controlling mechanisms. There is great need of uniform law and international co-operation to prevent and control cyber hacking worldwide.

अध्याय 2
Chapter 2
Cyber Fraud

Notes :

2.1 Introduction:

Cyber fraud refers to any type of deliberate deception for unfair or unlawful gain that occurs online. The most common form is online credit card theft. Other common forms of monetary cyber fraud include no delivery of paid products purchased through online auctions and no delivery of merchandise or software bought online.

Criminal activity involving the perpetration of a fraud through the use of the computer or the internet can take many different forms. One common form includes "hacking," in which a perpetrator uses sophisticated technological tools to remotely access a secure computer or internet location. A second common criminal activity involves illegally intercepting an electronic transmission not intended for the interceptor. This may result in the interception of private information such as passwords, credit card information, or other types of so-called identity theft.

What is Computer Crime?

There is a great deal of talk today about "computer fraud" but there is no such thing as computer fraud. What is usually meant is fraud carried out using a mouse of computer rather than traditional methods of paper and pen. The computer is simply the mechanism for perpetrating the fraud. Credit card Frauds are commited in India. Who says Indian Cyber Crimes are still in the Infancy? This is a man who penetrated the E-commerce for his personal benefits to a great extent. ATM Cards penetration in India. ATM card is the useful instrument in the era of computerization. All the banks are running behind the ATM Networks but are they really aware of the devils of the ATM cards?

Cyber Extortion:

An executive from Gujarat Ambuja Cement Ltd. played a mischief by posing himself as a girl and various other entities and duped the Abu-Dhabi resident for huge sums. Cyber Stalking This is a new concept that is being born on the Indian Horizons. First case was registered for Cyber stalking but not under the Information Technology Act. India's First Nigerian 419 Scam: The advance fee fraud which is also termed as the Nigerian scam, where the chain letters seeking help are sent and the citizens of various nations are conned. Hackers send ICICI bank and CITI bank customers unsolicitated e-mails and the sensitive and personal information is collected by simple techniques.

The most complex challenges faced by the Government and law enforcement agencies since 1960s in the cyberspace are cyber fraud and other Cyber Crimes. This may be because the business world, financial sectors etc were the most popular users of computer and internet from the early times of new multimedia technology.

The cyberspace becomes a media for the fraudsters where victims generally cannot recognize the accused. Therefore, cyber frauds become the most pervasive form of white collar crime worldwide. On 7th April 1999, the online financial message of 'yahoo! Inc.' was posted 'buyout news' that the 'pair gain' was being taken over by an Israeli company. Immediately after this news the company's publicity traded stock shortcoming was more than 30%. Subsequently the false story came out publicly. But by that time the company suffered significant financial loss and this incident caused financial loss to many investors too. This is one instance of online fraud. The accused Raligh of the North Carolina was arrested by Federal Bureau of Investigation (FBI) through an internet protocol address which was used by the accused. The accused was thereby charged with securities fraud.

On 5th March, 2000 about 19 people were charged for chat room fraud which caused about $8.4 million loss in New York. In India instance of Pune based Business Processes Organizations (BPO) fraud on April 2005, Karan Bahrees cyber fraud case came to light on June 2005. These are instances that cyber fraud is increasing day by day and there is an immediate need to prevent and control this complex problem worldwide. Another significant problem in cyberspace is unspecified and undefined jurisdiction. Therefore, application of laws, rules, and regulations are in shambles in world today.

2.2 Definition of Cyber Fraud:

The term "cyber fraud" is not defined in the Information Technology Act 2000 in India. However, according to D. Bainbridge, the phrase 'Computer fraud' is used to describe 'stealing money or property by means of a computer that is using a computer to obtain dishonestly, property including money and cheques, credit card services, or to evade dishonestly some debt or liability. It might involve dishonestly giving an instruction to a computer to transfer funds into a bank account or using a forged bank card to obtain, money from a cash dispenser i.e., automated teller machine'.

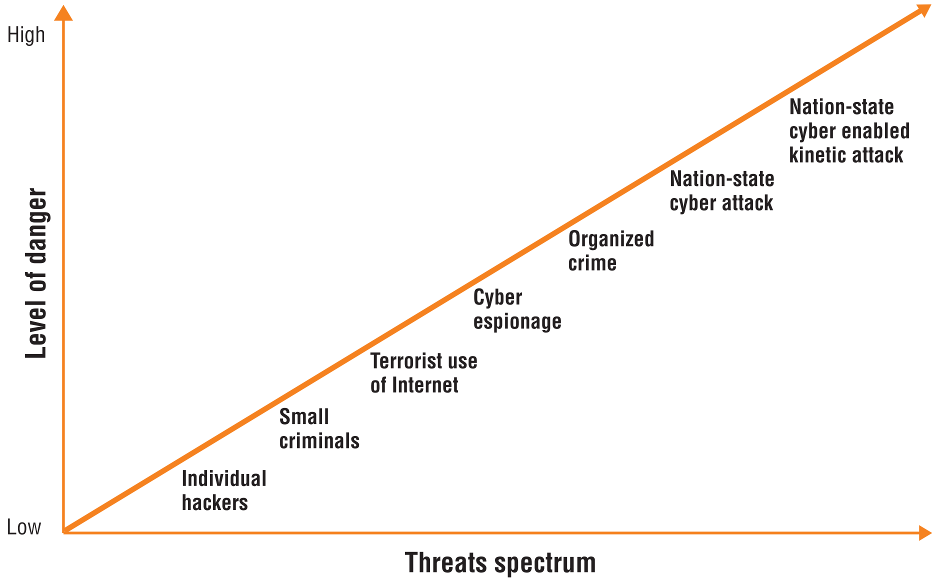
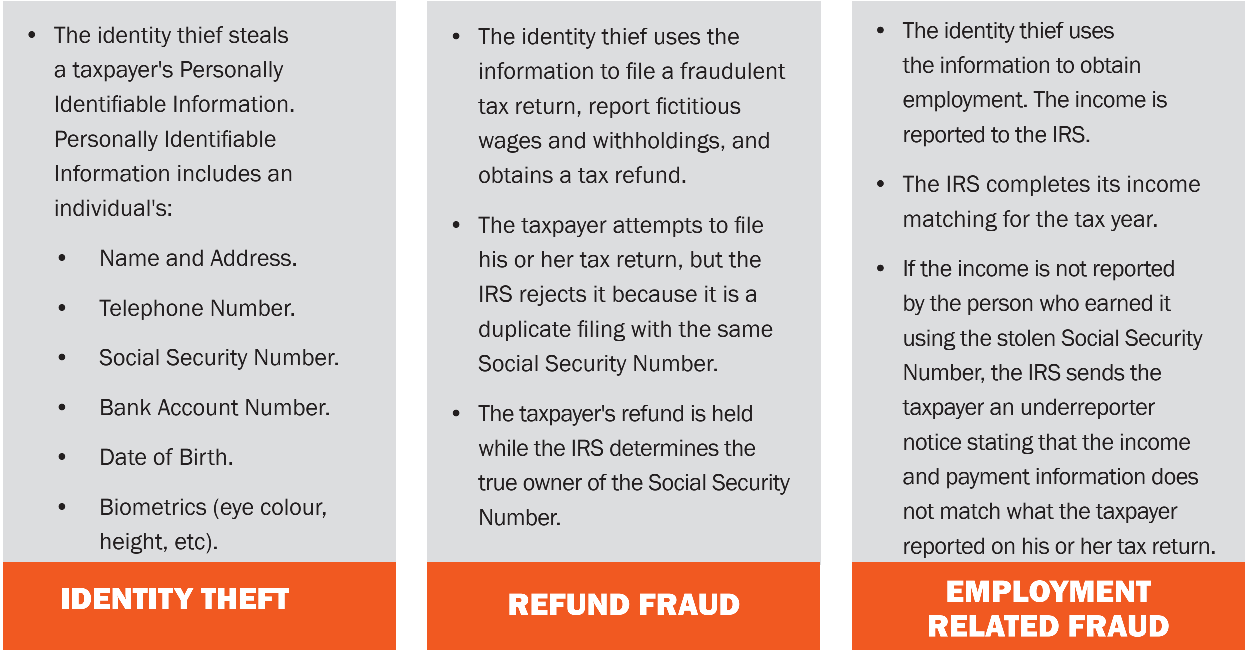


Fig. 2.1. Cyber Threat Spectrum

The term 'fraudulently' is defined in the Indian Penal Code 1860, s. 25 that a person is said to do a thing fraudulently if he does that thing with intent to defraud, but not otherwise. So, intention to defraud is very important i.e. *mens rea* or guilty mind and to do a thing is *actus reus* or human conduct. Following figure explains about Identity theft, Refund Fraud and Employment Related Fraud.



- The identity thief steals a taxpayer's Personally Identifiable Information. Personally Identifiable Information includes an individual's:
  - Name and Address.
  - Telephone Number.
  - Social Security Number.
  - Bank Account Number.
  - Date of Birth.
  - Biometrics (eye colour, height, etc).

IDENTITY THEFT

- The identity thief uses the information to file a fraudulent tax return, report fictitious wages and withholdings, and obtains a tax refund.
- The taxpayer attempts to file his or her tax return, but the IRS rejects it because it is a duplicate filing with the same Social Security Number.
- The taxpayer's refund is held while the IRS determines the true owner of the Social Security Number.

REFUND FRAUD

- The identity thief uses the information to obtain employment. The income is reported to the IRS.
- The IRS completes its income matching for the tax year.
- If the income is not reported by the person who earned it using the stolen Social Security Number, the IRS sends the taxpayer an underreporter notice stating that the income and payment information does not match what the taxpayer reported on his or her tax return.

EMPLOYMENT RELATED FRAUD

Fig. 2.2. Guidelines — Identity Theft, Refund Fraud, Employment — Related Fraud

2.3 Different Modes of Cyber Fraud:

2.3.1 Cyber Fraud due to Victim's Excitement:

Victim's excitement is one easy way to commit cyber fraud. Most of the times, victims are attracted and motivated to facilitate the schemes in cyberspace e.g., cyber marketing, e-banking, e-shopping and the like. These schemes are most of the times much misleading and victims are excited to these.

2.3.2 Personal Identities and Password Fraud in the Cyberspace:

Cyber criminals have learned that it is easier, less risky, and more rewarding to steal money through identity theft than it is to conduct more traditional crime such as an armed hold-up of a bank. Internet users should be acutely aware of the real dangers from cyber criminals that lurk when you open innocent-looking emails, conduct online banking, shop online, or even access social media networks. Identity theft includes stealing of personal information that enables cyber criminals to impersonate someone else. The more personal the information a cyber criminal collects on their victim, the more susceptible the victim is to the criminal stealing their money. In cyberspace the offenders pretend that they are good friends of victims and they try to convince victims with intention to access their personal information so that these can be used by the accused to commit cyber fraud i.e. credit card withdrawal, fraudulent money transaction, bank account fraud, ATM fraud etc

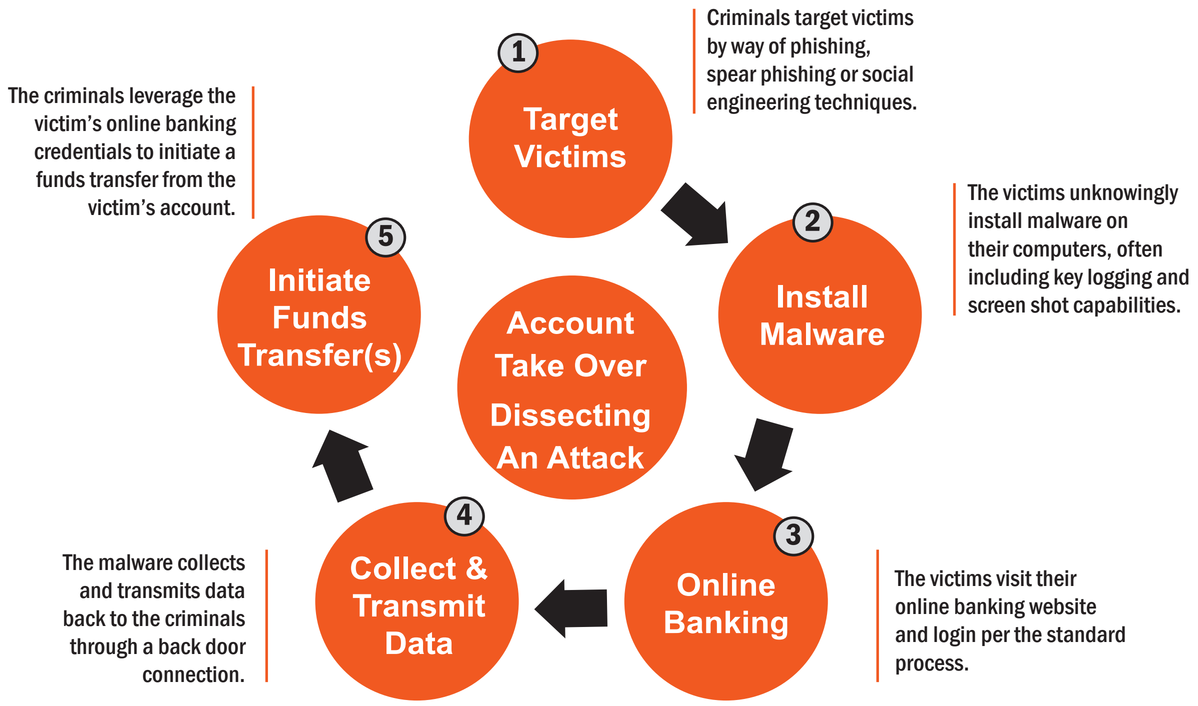

1
Target Victims
Criminals target victims by way of phishing, spear phishing or social engineering techniques.
2
Install Malware
The victims unknowingly install malware on their computers, often including key logging and screen shot capabilities.
3
Online Banking
The victims visit their online banking website and login per the standard process.
4
Collect & Transmit Data
The malware collects and transmits data back to the criminals through a back door connection.
5
Initiate Funds Transfer(s)
The criminals leverage the victim's online banking credentials to initiate a funds transfer from the victim's account.
Account Take Over
Dissecting An Attack

Fig. 2.3. Stages in Cyber Fraud

2.3.3 Cyber Fraud by False Representation:

The offenders in cyberspace also represent falsely that they have authority to do something for or on behalf of the victim/victims or they are the government officials. By this way they access the personal identity and commit cyber fraud.

2.3.4 Cyber Fraud Using Urgency:

"Urgent" is the term the fraudsters often use with some advertisement or statement which shows scope to win prize if invested by the potential victim or victims.

2.3.5 Cyber Lottery Fraud:

Cyber lottery scheme is one way to commit cyber fraud which require investment in tickets to give chance to win prize. It may also be called as cyber gambling.

2.3.6 Credit Scheme Fraud in Cyberspace:

Currently there is no generic system for identification in cyberspace. It is not possible to absolutely identify an entity or to accurately tell whether an object has a specific characteristic. Digital environments have inherent differences from real space which causes this discrepancy, and when implementing an identity system for cyberspace one needs to consider more than just the architectural nature of the system — any system chosen will have social repercussions which also need to be taken into account.

Identity is a unique piece of information associated with an entity. Identity itself is simply a collection of characteristics which are either inherent or are assigned by another. The colour of a person's hair and whether or not another thinks he is attractive is part of a person's identity.

Interactions done in real space inherently carry the identity of the person originating the transaction. Generally, physical traits are carried along in a transaction — for example when one purchase a book from a book store, the book dealer may remember the buyer's face or build. Credit scheme to offer loan in exchange of fees, interests, taxes, service charge etc. is one way to commit cyber fraud.

2.3.7 Travel Related Scheme:

Cyber shopping, telefunding, telemarketing etc. are also ways to commit fraud in cyber world.

2.3.8 Electronic-Mail Fraud and Internet Fraud:

On January 2005, a mass e-mail was posted to help Tsunami disaster victims but it was in fact a way to spread computer virus, to initiate a Denial of Service attack against a German website. The worm appears was "Tsunami donation! Please help!" which also invited recipients to open an attachment called "Tsunami.esec". If anyone opens it then it will forward the virus to other internet user. Innocent users were into a belief that they are helping for Tsunami disaster. Don't be the victim of a scam. If it sounds too good to be true, it probably is. The results of these scams can include: Identity theft, fraud, theft from your bank account or credit card, and computer viruses.

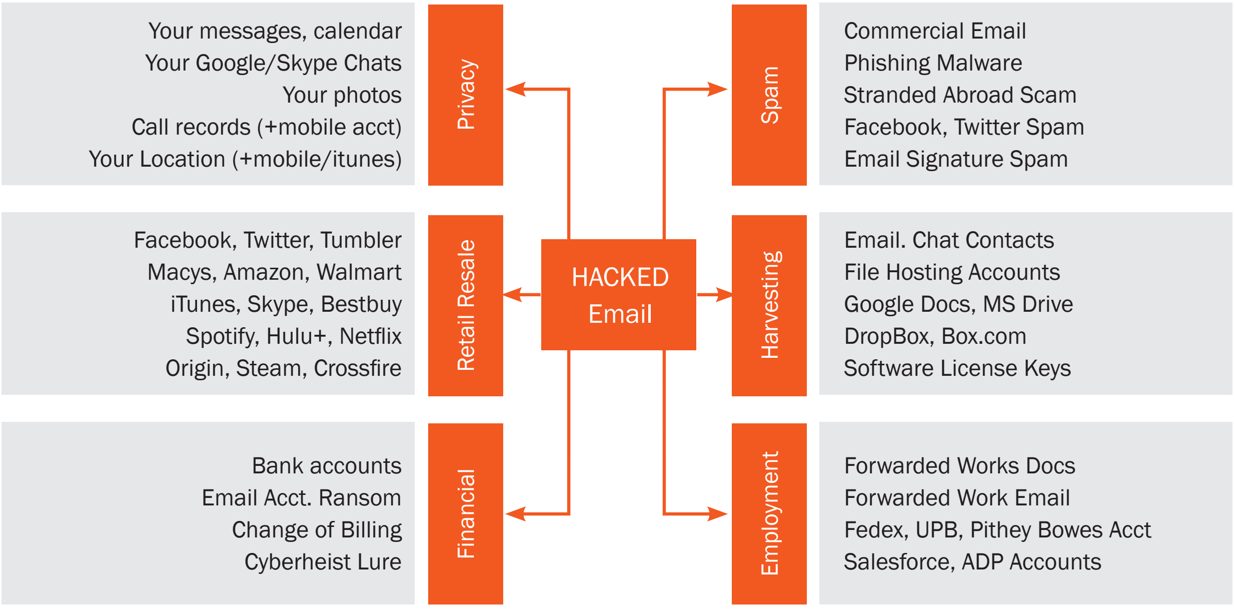


Fig. 2.4. E-mail Hacking Effects on Several Domains

2.4 Cyber Fraud in India:

In contemporary era of communication convergence, online money transaction, e-banking, e-shopping, internet auction, internet lottery, data conversation, data transfer to online ticket booking and in almost all aspects of our life, we have to walk on the superhighway. So, we have to go through cyberspace.

*"You have to grow from the inside out. None can teach you, none can make you spiritual. There is no other teacher but your own soul." - **Swami Vivekananda***

Due to liberalization and globalization India is also now well equipped to face e-commerce and e-governance. As in natural world, in cyber world also we are facing challenge from criminals and that is why India has adopted several security measures, enacted the Information Technology Act 2000 and Rules 2000; as well as constituted several bodies e.g., NASSCOM and Cyber Crimes Cell in several states for example in Delhi, Kolkata, Mumbai, Bangalore, Pune and Hyderabad. Like other crimes cyber fraud also is increasing day by day.

Nowhere it is safe whether the UK, the USA, Russia, Canada, Israel, Australia, Pakistan, Bangladesh or India. Though we do have our own laws, the jurisdiction in cyberspace cannot be defined or specified and it has become the cause of causes the major problems in cyber world.

2.4.1 Socio-Legal Impact of Cyber Fraud in India:

Impact of Cyber Laws in India: Cyber Law is a term that encapsulates the legal issues related to use of Communicative, Transactional, and Distributive aspects of networked information Devices and Technologies. It is less a distinct field of law in the way that property or contracts are, as it is a domain covering many areas of law and regulation. Some leading topics include Intellectual Property, Privacy, Freedom of Expression, and Jurisdiction. In Indian law, Cyber Crime has to be voluntary and wilful, an act or omission that adversely affects a person or property. The IT Act provides the backbone for E-Commerce and India's approach has been to look at E-Governance and E-Commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the security aspects.

CASE STUDY ▶ ***15: Pune Cyber Fraud Case:*** About 16 accused were arrested in the incident of Pune cyber fraud. Young employees of BPO industry Mphasis, Msource were the accused. They defrauded the United States based Citibank customers of more than Rs. 1.5 crore, including damage to data. John Varghese a 31 years young Bangkok returned to his Pune resident with new car, mobile, jewellery, and handy camera. He was the master mind of the story. Accused e.g. Miss Mourlene Fernandes (25 years), Ivan Thomas (30 years), Bijoy Alexander (26 years), Stephan Daniel (24 years), Siddhantha Mehta (20 years) and others were good friends of J. Varghese. The accused were authorised to access the confidential information of Citibank account holders as the bank provided e-banking service providers.

The two main accused Miss M. Fernandes the unit supervisor and Mr. Ivan Thomas the former Customer Care Executive accessed password/PINs information from about five account holders. It was just like taking house keys from owner by thieves. Thereafter the culprits had started their operation by sending and diverting e-mails of e-banking funds transactions. The victims were only receiving about funds transfer nothing else. One of the victims then lodged complaint to the Citibank and then Citibank alerted the Mumbai and New York City Investigative Services about the same. Mumbai Citigroup immediately reached recipient banks in Pune and alerted the Pune Police's Cyber Crime Cell to trap the cyber fraud. The accused were caught red-handed while they were about to check the fund transfer in a Rupee Co-operative Bank, Pune. Here one thing is to mention that the BPO arm of Mphasis Ltd., Msource did not file any complaint against this major cyber fraud case committed by their employees. The accused were charged under ss. 65, 66, 71 and 72 of the Information Technology Act 2000 and ss. 420, 465, 467 and 671 of the Indian Penal Code 1860.

CASE STUDY ▶ ***16: Cyber Fraud in West Bengal:*** In the State of West Bengal, Kolkata Police raided about 792 online lottery units and seven district units on 19th December 2004. The State Finance Department sought police force on 17th December to control violation of the Lotteries Regulation Act 1998, section IV i.e., the Central Law. The Police seized about 472 electronic lottery devices in Kolkata and investigated that most of them do not have trade licences. Vice-president of Play-wing said that they never violated rules. Website named http//:www.sushmitasen.com was misused by an accused in Toronto. Not only that websites http//:www.amitabhachchan.com, http//:www.hrithikrashan.com etc, were misused by cyber squatter and most of the times they used those domain names to facilitate pornography.

CASE STUDY ▶ ***17: Click Fraud:*** This is a kind of cyber fraud related to clicking on web search advertisements by users who have no aim to do business with advertisers. In web the company who puts the advertisement has to pay for each click by users to the web-search providers for example, Google, Yahoo and Rediffmail etc These web-search providers, therefore, use machines and people to make more clicks on advertisement without any aim to end the same and for which they will earn money from the advertisers.

CASE STUDY ▶ ***18: Hyderabad Rs. 20 Crore Data Conversion Fraud:*** Mr. C. Suresh the Managing Director of Vinsri Infotech and owner of the website InfoTech Pvt. Ltd. had started his business of data conversion in 1997, to give data entry works; to provide services of data entry, medical transcription, management and e-Books etc In 2002 January he fraudulently received Rs. 2.5 lakh (appx.) non-refundable deposits from each of the clients giving false promise to give data entry work. And on February 2003, when cheques issued to his clients by him were not cleared rather dishonoured because funds were not available; his clients started demanding either refund of their deposited amount or clearance of their bills and to provide work. But Mr. C. Suresh, the accused was silent. Therefore, his clients (about 1,500) went to police and lodged separate complaints. Then he was arrested from Secunderabad on the charge of cyber fraud i.e., about Rs. 20 crore data conversion fraud.

The Central Crime Station (CCS) investigators said that six more cases have been registered on cyber fraud and again police have identified at least 20 fake data conversion companies after this incident. Even in the branch offices the brokers collected falsely Rs. 10,000 to Rs. 50,000 from each client by giving such false promises.

CASE STUDY ▶ ***19: Karan Bahree's Case:*** The sting operation of the British Tabloid through their newspaper 'The Sun' seemed Indian BPO industries very cloudy in the end of June 2005. The lawyers and experts then became very busy to protect the security system of Indian BPO industries because they had the data transfer contracts with Desi Call Centres in India.

Surprisingly, Tim Pullan the law firm partner said from London that his Indian clients who were running call centres were satisfied with required security standards whether at New Delhi, Kolkata, Bangalore, Mumbai and in other cities. He again said that his firm had 7 biggest deals during the last 2 years in India and Indian companies had been willing and able to prove that they complied with ISO 799 i.e., Internationally recognized security standards, and BS 7799 i.e., the UK equivalent with the ISO security standards.

On 24th June 2005, a Journalist of 'The Sun' newspaper expressed that he had obtained account numbers, secret passwords, credit card details etc of almost 1000 British Bank customers from Karan Bahree the employee of a BPO firm at Gurgaon by paying 3 pounds. This 24 years old Mr. Karan Bahree was employed only before 3 months of the incident on probation as a Junior content writer with infinity e-search. He did not have authority to access those confidential information said by his employer.

Subsequently, Karan was fired from the job. Karan with co-accused Sameer delivered a Compact Disk (CD) to Mr. Oliver who was from the UK as the undercover reporter of British Tabloid Newspaper. But, no complaint had been registered to control and punish this culprit with the economic offence wing of the Delhi Police.

However, T.K. Kurien, CEO of Wipro BPO from Bangalore said "prosecution must be tight. The reality is that this crime has happened within our country and hence it must be treated as a criminal offence. The level of quality control must be the same as if it is in the client's location. Punishment could also be similar to that of a client location or perhaps even more stringent."

After Karan Bahrees case in June—July 2005, Prime Minister Dr. Manmohan Singh directed NASSCOM to amend and adopt more effective Data Protection Laws, security measures and to increase penalties for Cyber Crimes in superhighway with the tune of the UK, the USA and to adopt International standard of security system to prevent these instances in future.

The NASSCOM President Kiran Karnik said "the Internal Systems and processes can take care of data protection upto say 99% but 1% can result in what has currently happened. Our concern is to ensure that such persons are caught and punished promptly so that we set a very high".

It is very uncomfortable situation in India that those companies are very reluctant to such serious crimes; they do not lodge complaint and even do not inform police about cyber fraud. May be they are keeping quiet to protect their reputation in International market in the era of globalization and liberalised e-commerce and communication convergence. And in this regard our Information Technology Act 2000 is hopeful to some extent.

Section 80 empowers police officer not below the rank of Deputy Superintendent to take *suo motu* action for any reasonable and logical conclusion and to establish criminality on the ground of "reasonable suspicion" that accused has violated the provisions of the Act of 2000. Then it will become the cognizable offence. But this section is now omitted.

However, in this regard our law is not sufficient so far as the rank of police officer. The rank must be even below the Superintendent of Police. Because in Indian circumstances, we do not have sufficient staff to search, seize or take other investigative steps for even natural world crimes. And where they are in higher rank they are again very few in number which is insufficient to combat the crimes to maintain law and order in contemporary ever conflicting and ever changing society. Karan Bahree's case was dealt with under ss. 43(b), 65, 66, 72 and 74 of the Information Technology Act 2000.

The Prime Minister Dr. Manmohan Singh said "Indian professionals have built for themselves an enviable global reputation through hard work, dedication and commitment, and the occasional misguided acts of some individuals should not be allowed to damage the high reputation of all professionals."

CASE STUDY ▶ ***20: Bangalore Cyber Fraud Case:*** The Sutra Solutions case at Bangalore City with 42 branch offices were working as Call Centres and had taken more than 400 students and others promising them to give jobs after a few months. They were taken as trainees. The Sutra Collected Rs. 6,000 as customer support and Rs. 25,000 for technical support from trainess total Rs. 1.2 crore from all. After depositing the said money some of the trainees identified that the Sutra's website named www.sutrasolutions.com was going down, they were not paying building rent and telephone rents were due. Thereafter the victims lodged complaints against the company. Ajay Shah (CEO) had been absconding and the police arrested Mr. Raju Krishnamurthy on the charge of cyber fraud though thereafter he was released on bail.

CASE STUDY ▶ ***21: New Delhi Online Traders Case:*** One breaking news published by *Times News Network* alarming people about hackers whack online trading of shares. The CBI controlled this case of Cyber Crime where the password of a Ghaziabad based online trader was hacked by a hacker and caused loss of about Rs. 5 lakh.

The traders were frequently cheated by such hackers who got traders accounts information and misused it by bringing shares at very high prices and subsequently selling those share at very low prices causing financial losses. In Ghaziabad case, the 'cyber-breaking' was noticed when debt became Rs. 5 lakh against traders account. This was registered on 29th June by the CBI under s. 419 of the Indian Penal Code 1860 and s. 66 of the Information Technology Act 2000. The hacker invested Rs. 5 lakh from victims account to his own account. The Cyber Crime Cell of the CBI arrested 2 accused at Bhavnagar, Gujarat.

CASE STUDY ▶ ***22: Bangalore Cyber Fraud, June 2006:*** The accused Kashmiri was a resident of Bangalore who joined HSBC on 12th December 2005 by producing forged certificates. He had links with terrorist groups and the underworld groups. He and co-accused Nadeem were arrested on charges of data theft and cyber fraud. They committed data theft to illegally transfer money from account of a multinational and the UK based Bank's customers. HSBC electronic Data Processing India Pvt. Ltd., Bangalore was the Bank's BPO arm. They had lodged a complaint with the Cyber Crime Police Station (CCPS) against that cyber fraud.

Complain is the work of cowards! Braves took over the task of preparing the way! ***- Sardar Vallabhbhai Patel***

Immediately Kashmiri's friends and relatives of the accussed at Bangalore were traced by police team of economic offences and they found out that Kashmiri had three mobiles and from one of those he committed this crime.

The crime was so dangerous in nature that the HSBC's technical team from Hyderabad as well as Interpol section of police department became involved to investigate and control it. Between 14th March and 3rd April, Kashmiri and Nadeem committed this fraud which had an international dimension. After 3rd April Kashmiris identity was plugged by HSBC and he was suspended on 14th April. By that time Kashmiri committed data theft, passed information to others, transferred money from account holders of Bank and got the Payment.

CASE STUDY ▶ ***23: Kolkata Cyber Fraud Case, September 2006:*** Sulagna Roy a 23 years old NIFT educated call centre employee in a salt lake sector V call centre Jaishree Info Tech committed cyber fraud through calcuttaweb.com. Her nature of work was selling dish TV to the US clients. During her work she collected credit card information of those clients and then started purchasing more than 52 items worth Rs. 1.8 lakh ($4,000) by using laptop internet and cyber cafes Internet. These items includes jewellery, sarees, chocolate, air-conditioner etc

The calcuttaweb.com provided details of purchases to Detective Department and CID at Kolkata. She only earned Rs. 8,000 monthly but bought valuable things about which her mother was silent. She was arrested from her Behala home at Kolkata and was charged with fraud and cheating. She confessed that she did it for fun but not to commit any intentional crime. The City Court remanded her in police custody for 12 days.

Gyanwant Singh (DD) said "A California-based firm, Sys Soft Corporation, informed us that they do e-commerce in Kolkata through a portal, calcuttaweb.com. It was flooded with complaints about fraudulent purchases being made through this site during July—August.

We were also told that all these purchases were made through credit card of the US residents. The American firm had to pay compensation to all the credit card holders".

CASE STUDY ▶ ***24: Lottery Fraud and Cyber Squatter:*** Most of the times we receive electronic mails information that we are going to win or we won a prize in a lottery. To receive lottery money, the recipients of letters or e-mails naturally sent their reply. As they will send reply again they will receive another e-mail asking information about bank accounts, mode of transactions they prefer and other confidential information. They do charge money as processing fee before that fund transfer. But that prize in lottery to recipient's accounts never happened and on the other hand his confidential information, bank accounts etc may be misused or abused for commission of other crimes. This is what we can say on line lottery fraud. It happened in South Africa in November 2004, where about 419 international lottery fraudsters were attempting to commit cyber fraud worldwide by sending false using e-mails to multimember recipients.

In this regard Mr. Muller a member of the World Lottery Association Security and Risk Management Committee said that approximately 80% Lottery Scam Organizations were South

*Don't look back – forward, infinite energy, infinite enthusiasm, infinite daring, and infinite patience – then alone can great deeds be accomplished. - **Swami Vivekananda***

Africa based who were attempting to commit the said offence. He said that perpetrators were not South African but they were using South African e-mail addresses for quick action.

2.5 Conclusion and Suggestions:

Communication convergence and new multimedia technology have become very popular in contemporary globalised and liberalised society. In 1960s, the US Defence Department started using computer network; thereafter computer network was used by academic and research institutions and eventually the USA invented ICANN and Protocol system.

Gradually cyber world became cloudy and complex due to its misuse and abuse by criminals. Business world is the most popular user of computer, computer network, computer software and other information process devices of modern times. Detection and investigation of Cyber Crimes is emerging as a problem due to unspecified and undefined jurisdiction in cyberspace.

Instead of filling a complaint, the employers and industries are keen to compromise. They must understand their responsibility to file complaint before police administration, Cyber Crime Cell, CBI or other appropriate authorities to prevent and control those serious offences which are the black spots in cyberspace.

In India, industries and individuals must adopt world standard security systems with anti-virus measures to protect themselves from financial loss as well as loss of reputation in the era of liberalization, globalization and communication convergence.

Those crimes not only cause financial loss but also affect our social progress. The Financial Services Authority (FSA) must be more active to assess the security system standards of Indian call centres.

Though from London, Mr. Tim Pullan said that Indian call centres are very keen to follow and maintain the strict measures for data protection with the same standard of the European Union and the United Kingdom. The call centres have agreed to follow high contractual terms and conditions, such as taking immediate actions, switch off the system immediately etc

With Indian Prime Minister Dr. Manmohan Singh, we must accept "Indian professionals have built for themselves an enviable global reputation though hard work, dedication and commitment and the occasional misguided acts of some individuals should not be allowed to damage the high reputation of all professionals." He also asked NASSCOM to take necessary steps and amend law to increase punishment for Cyber Crimes and to adopt data protection and security system to compete world standards.

However, many people suspect that Bahree's case is a sting operation to suppress Indian Industries with a bad reputation in growing competition worldwide. Therefore, to protect even reputation of Indian Industries and to go for world competition, we must adopt great standards of rules and regulations with data protection, security standards, secrecy etc to stop Bahree like incidents in future.

With Government polices and law, people of India have vital role to play if we wish to prevent and control cyber fraud. For example at the time of e-business, e-shopping or e-banking while personal information along with credit card numbers are required or asked; we must apply our mind. Sometimes, we give all our information even money as processing fees but in reality we never receive any home delivery or otherwise from those fraudsters rather often they use our credit cards and other identities to fulfil their end.

अध्याय 3

Chapter 3

Cyber Pornography

Notes :

3.1 Introduction:

Addiction to pornographic material affects the rational thinking of the young and the old. The high proliferation of computers and broadband connections across the nation paved the way for easy access to websites that deal with such unhealthy practices. It is not an isolated incident occurring in America. Actually, internet porn is spreading like a wildfire across continents. The rehabilitation facilities have a tough time trying to combat the scenarios that facilitate the enjoyment of pornographic websites. A good share of the American teenagers has admitted that they have watched such obscene content with friends/fellow family members! What are the peculiarities of pornography addiction? For starters, it is very difficult to diagnose the condition. The other forms of problems such as the addiction to drugs or alcohol can be recognized very easily. We can avail timely aid to the participants by committing them to a rehabilitation facility. However, in pornography addiction, only the entity will know about his or her weaknesses! Yes, their friends or co-workers might know about this habit and might even try to exploit it for their satisfaction. There exist distinct differences between addiction to sex and addition to pornography.

The former requires the addict to seek multiple sexual partners to fulfil their desires. However, the only requirement to be hooked up with this addiction is to have access to pornographic material (via the internet or from friends) and lots of free time. Those who display interest in porn also engage in compulsive masturbation. How does this crop up as a major embarrassment? The addict might lose interest in their spouse. They disregard their education or daily duties to engage in pleasurable activities. Sometimes, pornographic addiction can camouflage itself into sex addiction. Lack of interest in the routine activities to participate in self-enjoyment sessions — all these are the typical symptoms of addiction to pornography. Following figure shows how a person can get addicted to Cyber Pornography (Fig. 3.1).

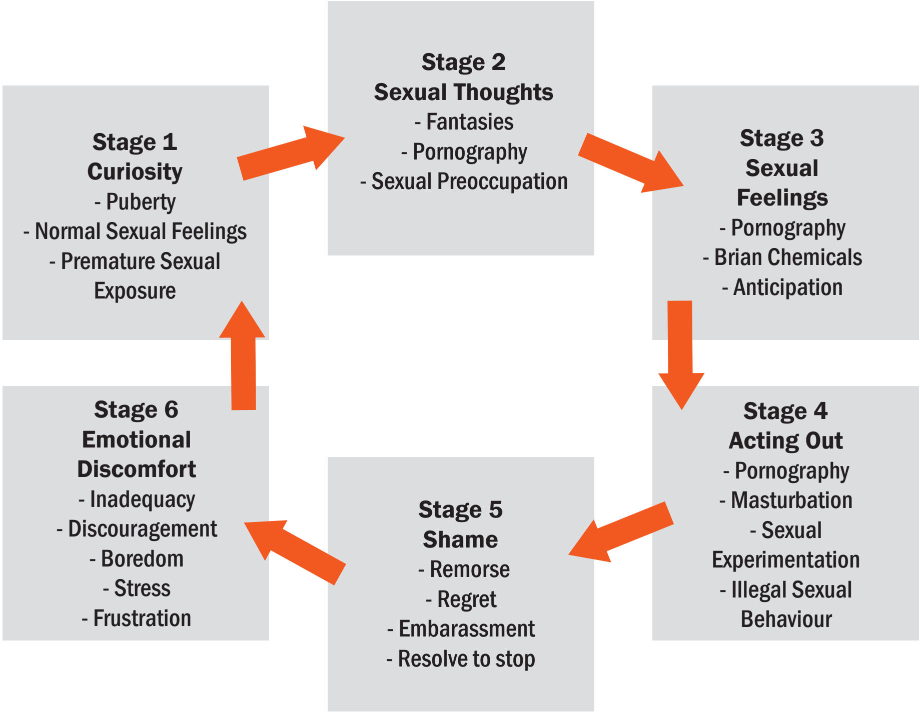


Fig. 3.1. Stages — How an Individual is Slowly Addicted to the Cyber Pornography

Nationality is respectable only when it is on the defence, when it is waging wars of liberation it is sacred; when those of domination it is accursed. ***- Sir Rabindranath Tagore***

A deep sense of guilt begins to materialize within the mind of the addict. However hard they try to control their urges, they yield to it in a day or two. Even if they make commitments, they fail to keep them. Expert treatment for pornography addiction is available with some of the rehabilitation centres. The primary factor is to neglect the "what would the others think of me, if they realize that I am addicted to porn" thoughts that linger in the mind of the addict. I realize that it can be hard for some of you.

Estimates suggest that up to 90% or more youth between 12 and 18 years have access to the Internet. Concern has been raised that this increased accessibility may lead to a rise in pornography seeking among children and adolescents, with potentially serious ramifications for child and adolescent sexual development. Using data from the Youth Internet Safety Survey, a nationally representative, cross-sectional telephone survey of 1501 children and adolescents (ages 10—17 years), characteristics associated with self-reported pornography seeking behaviour, both on the Internet and using traditional methods (e.g., magazines), are identified. Seekers of pornography, both online and off-line, are significantly more likely to be male, with only 5% of self-identified seekers being female. The vast majority (87%) of youth who report looking for sexual images online are 14 years of age or older, when it is developmentally appropriate to be sexually curious. Children under the age of 14 who have intentionally looked at pornography are more likely to report traditional exposures, such as magazines or movies. Concerns about a large group of young children exposing themselves to pornography on the Internet may be overstated. Those who report intentional exposure to pornography, irrespective of source, are significantly more likely to cross-sectionally report delinquent behaviour and substance use in the previous year. Further, online seekers versus offline seekers are more likely to report clinical features associated with depression and lower levels of emotional bonding with their caregiver. Results of the current investigation raise important questions for further inquiry. Findings from these cross-sectional data provide justification for longitudinal studies aimed at parsing out temporal sequencing of psychosocial experiences.

In the new millennium, world is running with globalization, liberalization and communication convergence technology. With speedy development of science and information technology, the ugly face of crime chart is unfortunately rising higher to cause more and more human tragedy. People are becoming power-oriented and they are conscious about their freedom rather than duties to maintain moral standard, decency, law and order in society. Law confers rights and imposes duties and works as vehicle to maintain social security.

Morality has sociological and psychological aspects. Morality is individual’s perception due to which human beings accept certain things as good and reject certain things as bad in society. It is dynamic with dynamic society. It varies from person to person and society to society. What is immoral for one is not so to others or in other society. There is no yardstick to determine what things are moral and what are immoral.

Therefore, it is left to the judiciary as reasonable and prudent repository of moral standard in society. Law and morality are closely related. When there is synthesis between them in society, there will be no conflict and society will progress smoothly and fast. But all morals are not enforceable by law rather we have to make a balance and accept shared morality.

In Life Insurance Corporation of India v Prof. M.D. Shah in the year 1993, the court held that this freedom is basic and fundamental right of individuals which they acquire by virtue of birth as human beings; and in a democratic country any attempt to gag this right except under Art. 19(2) is violation of democracy and Art. 19(1)(a). Therefore, we can say rights are not absolute in this universe whether in the natural world or cyber world. Rights are subject to reasonable restrictions because without restrictions if rights are allowed it will ruin society.

The first World Congress was held in August 1996 at Stockholm. The prime issue of the Congress was Commercial Sexual Exploitation of Children. The World Congress discussed about visual or audio material which exploit children sexually. Due to easy access to worldwide web through new multimedia technology, cyber pornography and other Cyber Crimes are increasing every moment. These pose a complex challenge for the legislation and law enforcing agencies worldwide. It became very easy to use, distribute or sell pornographic materials. These acts affect moral and psychological growth of society.

Child abuse, sexual violence against women and other sexual crimes are the direct effect of pornographic images which are also causing breaking of marriage tie, juvenile delinquency and sexual diseases. In contemporary phenomenon World Wide Web has become the playground and game room. People are motivated more to chat room than healthy information. International treaties, co-operation and initiatives are taken by the European Union to combat possessing and distributing cyber pornography and computer related offences.

The United States of America (USA), the United Kingdom (UK), Canada, Russia, Australia, India and other countries worldwide are raising their voice to fight against cyber pornography which corrupts minds of young people and others who are sensitive to these. It demonises our socio-moral values, culture and taboos. It affects human psychology, which cause social violence, disturb law and order in society. It is the prime duty of criminal law to maintain social security, law and public order.

3.2 International Initiatives to Combat Cyber Pornography:

The European Council's 12th Conference of Directors by the Criminological Research Institute in the year 1976 discussed the issue of computer-related crimes. Thereafter several conferences, conventions and treaties followed their recommendations. In the year 1990, the United Nations Congress took special initiatives for the prevention of Cyber Crimes. Canada introduced a draft convention in this regard.

In the year 1994, a Manual on "The Prevention and Control of Computer-related Crime" was prepared and presented by the United Nations for review of Criminal Policy. The United Nations Economic and Social Council (UNESCO) took vital initiatives to combat online sexual

*"The immoral can no more earn respect Than the envious be rich."- **Thiruvalluvar***

abuse, child pornography and pedophilia and took initiatives to adopt uniform preventive and controlling measures specially on 18th as well as on 19th January, 1999 at Paris with 150 participants.

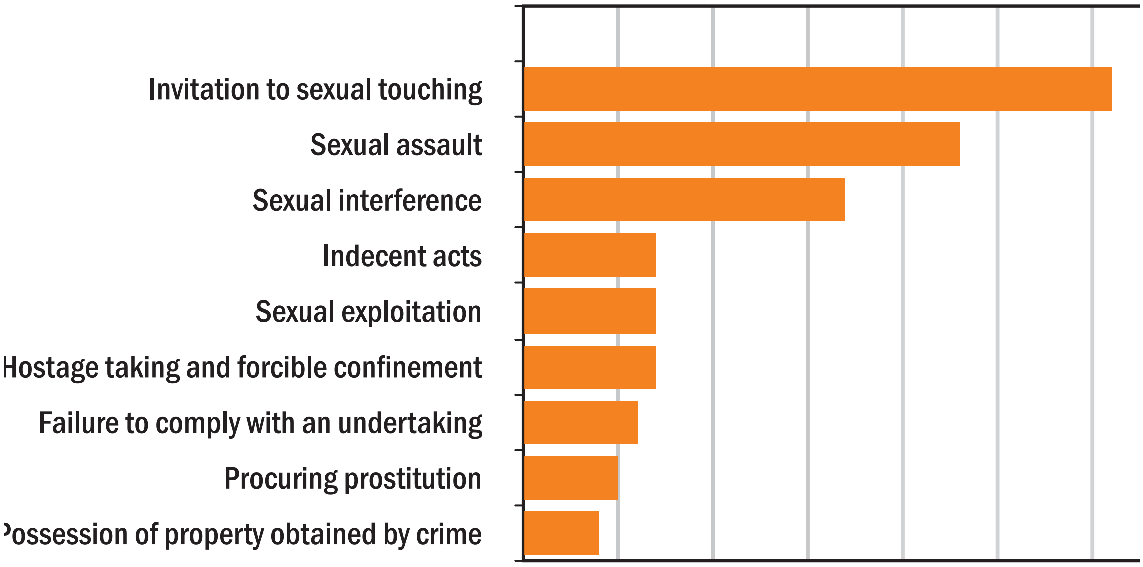


Fig. 3.2. Proportion of Child luring cases related to Cyber Pornography

In October 2000, the European Union and the United States of America initiated a draft which is the first draft of International Treaty on Cyber Crimes. The preamble of the treaty invites for international co-operation to combat the rapid growth of Cyber Crimes worldwide. The treaty specially invites initiatives and co-operation of the United Nations, the OECD, the European Union and the G-8 countries.

On 22nd June 2001, the European Council's Committee on Crime Problems approved the final draft of Cyber Crimes related convention during its 50th plenary session. Article 9 provides that

(1) Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

- producing child pornography for the purpose of its distribution through a computer system,
- offering or making available child pornography through a computer system,
- distributing or transmitting child pornography through a computer system,
- procuring child pornography through a computer system for oneself or for others,
- possessing child pornography in a computer system or on a computer data storage medium.

(2) For the purpose of above mentioned Paragraph-I 'child pornography' shall include pornographic materials which visually depict,

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. Realistic images representing' a minor engaged in sexually explicit conduct.

On 22nd April 2002, police reported about arrest of 25 people from the USA and 9 from the European countries for violating child pornography laws e.g., from Sweden, Switzerland, Denmark, Germany, Britain and other four European countries. This case is the instance of sexual abuse of children aged about 3 to 15 years both boys and girls. The Police investigation started worldwide from November 2001. At first Swedish Police traced an online photograph of a man who was abusing a girl of 11 years. Police found out on the shirt of that man a logo of a Danish company. Then, Danish police detected and arrested the man with his family and seized their computers which contained more photographs of those girls, the name of recipients and photographs from accused. They were sentence to imprisonment upto 8 years. But, they were released from jail during trial.

3.2.1 Brian Tod Schellenberg:

There was a report published as an international investigation into child pornography that 41 years old Brian Tod Schellenberg was charged with physical and sexual abuse of a six years old girl and an infant boy to create image so that it could be posted on internet websites. He was charged on four counts for sexual exploitation of children and on one count for possessing child pornography by the US District Court. Federal Bureau of Investigation (FBI) which was well concerned about protection of the victim's identities. The Special Police Unit investigation was initiated in Toronto, Canada and 5 children were taken into custody. Search warrants were executed in 5 States along with London, England and 5 offenders were arrested. Most horrific accused was Schellenberg who attempted to hire a man to kill the child victim and her mother. The Toronto Police Superintendent visited the unit. They found out images which were connected with North Carolina and posted to a 'shared secrets workspace'. This was used by 15 law enforcement agencies worldwide. The image contained physical as well as sexual exploitation and abuse of children. They found out more than a thousand such images in the home computer of the accused. The accused was then working for one software company. Police examined accused's computers and compact discs (CD's).

In connection with the same investigation, police found out another case where mother K. Henry was trying to arrange her own daughter to someone for sexual encounters. She was charged on one count for possessing child pornography and for transmission of objectionable and indecent material, by the US Court.

3.3 Cyber Pornography in the United Kingdom:

Though the United Kingdom does not have any written Constitution, their freedom of speech and expressions is recognized through several laws. As we know absolute liberty will ruin society; therefore, restrictions upon the exercise and enjoyment of those rights are imposed. Those restrictions are reasonable to maintain law and order in society.

Obscenity was criminalized about 304 years back. However in the year 1727 obscenity was treated as common law offence in R v Curl and period. In Regina v Hicklin case Lord Cockburn observed that 'think the text of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those, whose minds are open to such immoral influences and into whose hands a publication of this sort may fall.' This is popularly known as Hicklin test.

3.4 Prevention and Control of Cyber Pornography in India:

The Information Technology Act 2000 was enacted by adopting the United Nations Model Law to adopt a legal framework in Indian situation, to govern and regulate the internet or online transaction, electronic contract, digital signature and also to prevent and control Cyber Crimes. Cyber Crimes are crimes committed in superhighway using new technology such as hacking, phreaking, identity theft, cyber fraud, cyber pornography, cyber terrorism, flowing of viruses, tampering source code and the list is not exhaustive.

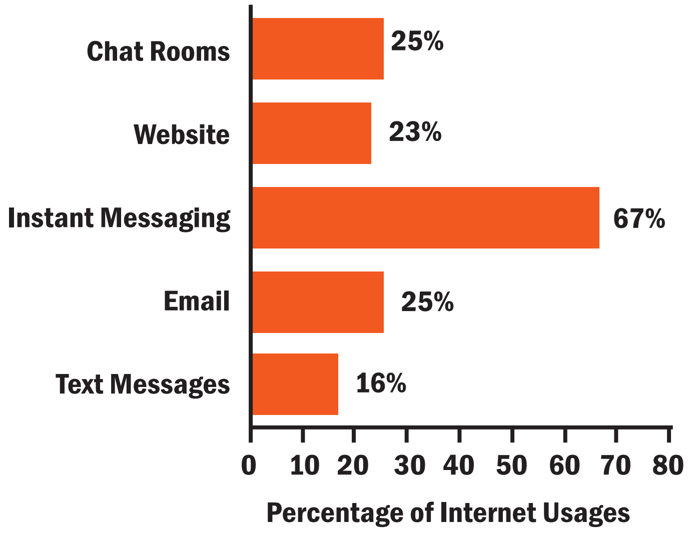


Fig. 3.3. Electronic Aggression in Distinct Applications

In the Information Technology Act 2000 in India, one full chapter deals with offences and few controlling as well as preventive measures in the Information Technology Rules. Specially s. 67 deals with cyber pornography in the form of flowing of obscene material/materials and it is punishable offence. This proposed amendment of the Act 2000 in the year 2006 suggested to amend s. 67 and to insert one new s. 67A. Herein we must refer not only to s. 67 of the Information Technology Act 2000 which criminalises obscenity rather before that in the year 1860 Indian Penal Code was passed where ss. 292, 293 and 294 prohibit obscene publications and s. 499 prohibits defamation. The Constitution of India, Art. 19(2) prohibits obscene, immoral and indecent speech, expression and publication.

3.4.1 Cyber Pornography and the Constitution of India:

The Constitution of India is the basis and supreme law in India. It guarantees in Art. 19(1) a freedom of speech and expression. It provides that all citizens have the right to freedom of speech and expression. Article 19(2) provides that in the interest of decency or morality, reasonable restrictions may be imposed by law upon this freedom.

In Preamble of Indian Constitution 1950, especially the words 'Democratic', 'Republic', 'Justice-social, economic and political; liberty of thought, expression, belief, faith and worship' show that we require balance between law and morality. For example in changing society we have due concern about changing art, literature, sculpture, architecture etc for development and progress of society which are very essential.

We can say in our Democratic and Republic India that we do have freedom and liberty to enjoy our life, to express our views in any way we chose but it is not absolute. Because we know, nothing is absolute in this universe there has to have limitations or reasonable restrictions otherwise absolute freedom will ruin our society.

Therefore, we the people of India while enacted and adopted our Constitution, we imposed upon ourselves certain limitations, restrictions, duties and responsibilities along with our rights to ourselves. Rights are very basic and sacrosanct. Freedoms are essential even to enjoy our very basic rights e.g., right to life and personal liberty under Art. 21 and there is no watertight compartment between several rights and duties rather all those Articles are related to each others with harmonious construction.

In case of violation of those rights we have remedies under Art. 32 by the Supreme Court of India and under Art. 226 by High Courts by way of writs and other proper reliefs. However, Art. 32 itself is a fundamental right in India. Because we know, rights without remedies are meaningless. We can reasonably enjoy those rights in cyber world too i.e., freedom of speech and expression along with limitations for which we have special law i.e. the Information Technology Act 2000.

3.4.2 Legislative Approach in India to Prevent and Control Cyber Pornography:

(1) THE INDIAN PENAL CODE 1860: The Indian Penal Code 1860, ss. 292, 293 and 294 provide for limitations and prohibitions of certain things which are obscene with some exceptional cases. Section 292 prohibits sale, distribution, publication, export, import etc of obscene books, pamphlets, papers, writings, drawings, paintings, representations and the like except justifications under this section e.g., literature, art, learning, monuments, etc and prescribes punishments on first conviction with imprisonment for a term which may extend to two years and with fine which may extend to ₹2,000, and on second conviction with imprisonment for a term which may extend to five years and also with fine which may extend to ₹5,000.

(2) THE INFORMATION TECHNOLOGY ACT 2000: The Information Technology Act 2000, s. 67 provides for the penal sanctions without mentioning exceptions as in s. 292 of the Indian Penal Code 1860 (IPC). Section 292 provides that the publication or possession of obscene material must be taken as a whole before imposing punishment. To protect child pornography, IPC provides special section under s. 293. Whereas s. 67 does not mention possession of objectionable material and the charge under this section can be brought if a part of the material is proved to be obscene.

3.4.3 Judicial Response before the Act 2000 in India:

Shaw v Director of Public Prosecution: In the UK, a magazine named 'The Ladies Directory' was related to distribute in market that contained names, addresses of prostitutes, pornographic photographs and descriptions of their practices. The accused was charged for such pornographic distribution in public as an offence because it corrupts the mind of people or individuals and this act was treated by court as 'a conspiracy to corrupt public morality'.

The judiciary referred here

i. John Stuart Mills principle of 'harm to others' mentioned in his book 'On liberty';

ii. the conclusion of the debate of H.L.A. Hart and Prof. Devline about enforcement of morality by law where they concluded with the need of balance between law and morals and shared morality; and

iii. the recommendations of the Wolfenden Committee's in the year 1957 in the UK which was similar to J.S. Mills principle.

The Wolfenden Committee's recommendations were that while prostitute and homosexual parties are two consenting adults and doing something within four walls without hampering others or without causing harm to others, the State shall not enter into individual's private liberty and the same activities will not be treated as crime.

Indian judiciary whole heartedly followed these principles as well as Hiclin Test and decision of the US Court in Roth's case. In Ranjit D. Udeshi v State of Maharashtra, the Supreme Court of India declared 'Lady Chatterley's Lovers' written by D.H. Lawrence as obscene book and publication. The Court held that there is difference between 'obscenity' and 'pornography'. Precise definitions are not possible. However, obscenity is any material, which tends to corrupt, cause annoyance, something of horror, indecent, immoral or with sexual tendency. 'Pornography' means any material in writing, picture or other form, which is intended to arouse sexual desire. Both are against public morality and decency.

Legislation which prohibits 'obscenity' and 'pornography' are laws with moral value and when there is synthesis between law and morality, the situation will be balanced with shared morality.

CASE STUDY ▶ ***25: Bobby Art International etc v Ompal Singh Hoon:*** Controversy about the film "Bandit Queen" which contained nude scene brought the Supreme Courts attention. The story dealt with the life of Phoolan Devi from her childhood in village till the period of brutal torture to her. She was kidnapped, gang raped by the dacoits and was sexually harassed. The film shows how she was raped in her early age and thereafter two minutes nude scene in front of villagers standing around her and she was paraded nude from her head to toe. Thereafter, when she joined the dacoits group, she took revenge by killing 20 Thakur's of her village. In that film the rapists obscene posterior was also shown in the rape scene.

CASE STUDY ▶ ***26: K.A. Abbas v Union of India:*** The Chief Justice of Supreme Court M. Hidayatullah and other Judges held regarding film censorship that our freedom of speech and expression is not absolute rather limited by reasonable restrictions under Art. 19(2) in the interest of general public to maintain public decency and morality. Therefore, film censorship has full jurisdiction in the field of cinematograph film to prevent and control obscenity and pornography.

CASE STUDY ▶ ***27: Samaresh Bose v Mr. Amal Mitra:*** The case was about 'Prajapati' controversy which was published in 'Sarodiya Desh' for the Bengal written by petitioner. Defendant was a young advocate at that time who complained that the novel contained obscene materials. Print, sale distribution and exhibition of the same which had tendency to corrupt public morals as described sexual feelings after viewing women's private visual body, described close emotional relations with friend's sister. Herein, court held that a novel written by a well known writer of novels and stories, by which the author intends to expose various evils and ills prevailing in the society with particular emphasis on the problems which affect society in reality, cannot be treated as vulgar writing and is not necessarily obscene.

CASE STUDY ▶ ***28: Sukanto Halder v State of West Bengal:*** Case was relating to magazine "Nara Nari" which was treated as an obscene publication. Therefore, to give effect to public morality above art, literature the court under s. 292 of the Indian Penal Code 1860 convicted the petitioner and sentenced him to two months rigorous imprisonment and a fine of Rs. 200 in default to rigorous imprisonment for two weeks.

CASE STUDY ▶ ***29: Raj Kapoor v State of Maharashtra:*** Issue was the most controversial film "Satyam, Shivam Sundaram". Justice Krishna Iyer held that 'A' certificate by a high-powered Board of Censors with specialised composition and statutory mandate is essential and acceptable. But we have to examine whether it breaches public morals and decency to invoke the penal provisions. However, certificate of the Board has evidentiary value but does not exclude criminal liability on publication of obscene and pornographic materials.

3.4.4 Judicial Response in India after the Information Technology Act 2000:

In Jayesh S. Thakkar v State of Maharashtra on 29th May 2001, the petitioners wrote a letter to the Chief Justice of the Bombay High Court. The complaint of the letter was about pornographic websites on the internet. The letter was treated as *suo motu* writ petition.

On 26th September 2001, the Division Bench of the Bombay High Court consisting of B.P. Singh, CJ and Dr. D.Y. Chandrachurd, J. passed an order to appoint a committee to suggest and recommend ways of preventing and controlling measure and means to protect children from access to pornographic and obscene material on the internet.

The committee considered several public opinions through Internet and other media and recommended in a report. The Bombay High Court Special Committee's report on Shielding Minors from Cyber-Porn i.e., Protecting Minors from Unsuitable Internet Material on 30th January 2002 was as follows:

EXECUTIVE SUMMARY:

(1) ***Site Blocking.*** The committee comprehensively rejected the proposal for site blocking as being technically and legally unsound.

(2) ***Cyber Cafes.*** The Committee's recommendations include:

a) A suggested definition of cyber cafes to be included in the rules under the Bombay Police Act.

b) Procedures for licensing cyber fares as none are as yet licensed or regulated.

c) Regulations requiring cyber cafe operators to demand photo identity cards of any kind from all users.

d) Requiring that minors be restricted to using machines in the common open space of cyber cafes i.e., not in cubicles.

e) Requiring that these machines be fitted with software filters.

f) Providing for the maintenance of internet protocol address allocation time-stamped logs for all machines in the cyber cafe network.

(3) ***Service Providers.*** The recommendations cover (a) requirements for maintenance of time-stamped logs of different descriptions; (b) requirements for synchronisation of internal clocks and connectivity authentication logs.

(4) ***Educational Measures.*** These include

a) electronic mail and website information to be provided by internet service providers informing the public about hazards and possible solutions.

b) Offering filters software to subscribers as an option.

c) Setting up a hotline to the Cyber Crime investigation cell.

d) Taking steps to increase awareness about Cyber Crime in general.

CASE STUDY ***30: Mumbai Housewife Harassed due to Cyber Pornography 2003:*** In Mumbai a housewife was receiving frequent filthy telephone calls, threatening her for sexual favour from one young boy in the city who got her phone number and name from an advertisement placed in a pornographic website in the Internet. Soon after the complaint filed by her husband Mumbai police traced out that she was not the only women who was harassed in this way and receiving such harrowing calls. Mumbai police traced that young boy who was the accused.

CASE STUDY ▶ *31: In Tamil Nadu v Suhas Katti:* This case was another significant step in the Indian law enforcement agencies where within 7 months of filing FIR, the conviction was achieved successfully. This was the first case of the Cyber Crime Cell Chennai. For this speedy disposal of this case, great assistance had been given by Naavi.com and the Cyber Evidence Archival Centre.

In this case Indian police had shown their ability as investigators by producing satisfactory evidence against the accused. The defendant was charged for annoying, obscene and defamatory message in the yahoo message group relating to a divorcee woman. The accused at first opened a false account in the name of the victim and then sent her information through electronic-mails. It annoyed the victim because she had to face harrowing calls.

In February 2004 the victim filed the complaint about the fact before police. The Chennai police traced the accused at Mumbai and arrested him immediately after a few days. It was found out by the police that the accused was victim's family friend, known to her and wanted to marry her. But she did not marry the accused. However, she married another one who ended it in divorce later on. After her divorce the accused again became very crazy about her and started contacting her but she refused for the same. Then the accused started harassing her through internet.

The charge sheet was filed against the accused under ss. 469, 509 of the Indian Penal Code 1860 and s. 67 of the Information Technology Act 2000 on 24th March 2004 before the Hon'ble Additional CJM, Egmore. There were 34 documents and other material objects and 18 witnesses were produced before the court by Chennai police with great help the Cyber Evidence Archival Centre of which 12 witnesses were examined on the side of prosecution.

On the basis of the expert witness, the court held that the crime is conclusively proved. On 5th November 2004 the court delivered the judgment that the accused was found guilty of offences under ss. 469, 509 of the Indian Penal Code and s. 67 of the Information Technology Act 2000. Therefore, the accused was convicted and was sentenced for the offence to undergo rigorous imprisonment for two years under s. 469 of the Indian Penal Code i.e, forgery for the purpose of harming reputation and to pay Rs. 500 fine; for the offence under s. 509 of the Indian Penal Code i.e., word, gesture or act intended to insult the modesty of a woman with one year simple imprisonment and Rs. 500 fine; and for the offence under s. 67 of the Information Technology Act 2000 with two years rigorous imprisonment and Rs. 4,000 fine. The court held that all those sentences must run concurrently. The accused was lodged at Central Prison at Chennai and he paid the above mentioned fine.

CASE STUDY ▶ *32: A MAN POSING AS A 15 YEAR OLD GIRL:* Through Internet chat room a 30 years old man represented himself as if he is a 15 years old girl before a 16 years old boy from 2002 to 2004. The boy then ran away from his home to his girl friend at Mumbai and discovered the truth. The accused, 30 years old man sexually abused the victim, stole money from him and beat him up. This was the result of chat room friendship which caused homosexuality which is prohibited under s. 377 of the Indian Penal Code 1860. Section 377 deals with unnatural offence it runs thus: whoever voluntarily has carnal intercourse against the order of nature with any man, woman or animal shall be punished with imprisonment for life, or with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

CASE STUDY ▶ ***33: Airforce Bal Bharti School 2001:*** The case was filed in the Juvenile Court, Delhi on the charge of cyber pornography. Some jurists say this is the first Indian cyber pornographic case which was charge sheeted in the Juvenile Court. The brief facts in issue were that a student of the Airforce Bal Bharti School, Lodhi Road, New Delhi was arrested by the Delhi Police in the year 2001 April.

The alleged accused was then a class XII student who created a pornographic website as revenge of being teased by classmates and teachers. He listed in that website the names of his 12 school mates' girls and teachers in sexually explicit manner. He was then suspended by the School Authorities though the juvenile court allowed his bail prayer. However, he was charged under s. 67 of the Information Technology Act 2000, and ss. 292, 293, 294 of the Indian Penal Code and the Indecent Representation of Women Act. The most significant steps were taken by the law enforcement agencies in India.

CASE STUDY ▶ ***34: Bhubaneswar Case:*** The Xavier Institute of Management lodged a Cyber Crime complaint with the police in December 2004 that students and staff of these institutions are getting numerous obscene electronic mails. Not only those, the students were afraid of online threatening, hacking and spamming. Police appointed technical experts to investigate and examine the whole technological matters. At first these indecent electronic mails were considered by them as spam mails. Gradually, the students and staff were being over flooded with obscene mails and continuous sexual harassment through internet.

At that time Bhubaneswar police was weak to fight against Cyber Crimes. Police Superintendent Mr. Amitabh Thakur said that police officers were not trained enough to tackle the case. However, they might ask for expertise from technical persons to tackle the situation according to the instruction of the State Crime Record Board.

CASE STUDY ▶ ***35: Aligarh's Cyber Cafes Case before the National Human Rights Commission, New Delhi:*** On 23rd December 2004, one Uttar Pradesh Policeman was recognized as pornography seeker. He humiliated young school girls in cyber cafes at Aligarh. A senior officer warned girls that they must not lose temper otherwise they may lose a great deal. Dialogues were mostly in Hindi, i.e., "Garmi Na Dikhao ... Garmi Dikhaogi to Bahut Kuchh Garam ... Jaye Ga".

That was not enough, police officer dragged one teenage girl by her hair and she was compelled to look into the news channel camera's lens. In India, even using real names and picture of girls who are arrested on the charge of prostitution is not allowed by law. One of the policemen also used filthy language by saying that now you are ashamed but you did not feel

Fill the brain with high thoughts, highest ideals, place them day and night before you, and out of that will come great work. Great work requires great and persistent effort for a long time. Character has to be established through a thousand stumbles. - ***Swami Vivekananda*** that when you had decided to bunk school to spend time with ... in Hindi i.e., 'Ab sharam aa rahi hai... Jab school se bhaag kar aayi thee to sharam nahee aa rahi thi'.

There were no women police at that time when police raids were carried out at cyber cafes. This case was the complete violation of human rights of those students specially violation of their right to live with honour and dignity. Therefore, the National Human Rights Commission took *suo motu* cognizance of reports in the print and media and asked the chief secretary and the Director General of Police, Government of Uttar Pradesh to look into the allegations by sending their comments within two weeks.

3.5 Conclusion and Suggestions:

New multimedia technology is being misused and abused by criminals in cyberspace. Cyber pornography, online child pornography, cyber spamming etc are increasing every moment. Cyber-pornography is not only national but also international legal challenge which needs intensive study, research and world-wide awareness.

We have right to privacy that more confidential and private information are to be kept in secret and undisclosed because we wish do not to disclose these to outsiders. The moment these are disclosed, they will lose secrecy, confidentiality and privacy. Right to privacy directly flows from Art. 21 of the Constitution of India. Though the very word is not written there, in case of violation of our privacy we can get judicial remedy. The same right is also protected under the Indian Penal Code.

MMS Clip or web camera clipping must come under the Information Technology Act 2000 and these are also to be treated as computer, computer system or computer network in wider sense. The Information Technology Act 2000 does not specifically provide the law of child pornography, MMS clip, video clip, use of web camera, spy camera and publication of obscene as well as pornographic material through internet etc because this Act was passed in a hurry and at that time these complex problems were raised and the law has been amended but still these anomalies are there in reality.

However, to solve contemporary problems in dynamic society, law must be interpreted in the dynamic way with liberal construction. Article 9 of the European Union's draft Convention prohibits cyber pornography. The Communication Convergence Bill 2001, cl. 70 also is not adequate in contemporary social scenario. This clause prescribes punishment for sending any content that is grossly offensive or of an indecent obscene or menacing character or for the purpose of causing annoyance, inconvenience, obstructing, criminal intimidation, enmity etc by means of a communication service or a network infrastructure facility, knowing that the content is false and for persistently making use for this purpose a communication service or a network infrastructure facility.

The proposed Information Technology (Amendment) Bill 2006, ss. 67 and 67A are hopeful to the extent that viewing cyber pornography in private place is not an offence but if it is done by any one in public i.e., in cyber cafe, public e-libraries etc are offensive. In s. 67, for the publication or transmission of obscene material in electronic form in cyber world, the punishment prescribed as two years imprisonment and fine up to five lakh rupees for first time offence and for second time or subsequent conviction with imprisonment which may extend up to five years or with fine up to ten lakh rupees. Relating to cyber pornography another section has been proposed to be inserted after s. 67 that is 67A which prescribes punishment for publishing or transmitting of material containing sexually explicit act or conduct in electronic form for first conviction imprisonment will be up to 5 years and up to ten lakh rupees fine and for second or subsequent conviction up to seven years imprisonment and up to ten lakh rupees fine. However, by the Amendment Act, legislature would increase penalty more to combat the situation as there was no hurry for amendment rather it was made after six years.

There are several means to view, produce, transmit cyber pornography, such as the Grand Theft Auto (GTA) apparently a video game which gives users access to hidden materials. Users can pick up girls of their choice and have interactive sexual activities using keyboard and mouse clicking after opening the patch called “Hot Coffee”. One can make a pornographic material in computer and then download in Multimedia Message Service (MMS) and circulate it. From one computer before MMS clip, criminals can copy images and send to other computer with new name of file and again it may be circulated with new name to mobile phone users and computer users. They can make a CD on it and sell the same. Such acts whether done at home or private place, affects society at large, therefore, these will be treated as illegal and punishable under s. 67 and proposed s. 67A of the Information Technology Act, as proposed to be amended in the year 2006.

So far the MMS clip of film actresses, were made, as they may be the effect of flop films which drugged them for reverse publicity so that their other films may not flop and MMS clips became an easiest way to bring themselves in controversy.

Suggestions

We require more teeth to the law to cope up with the situation. We need to adopt specific and clear definition of Cyber Crime, cyber pornography, and child pornography in cyberspace.

There is a need for teaching and training to law enforcing agencies, judiciary, intermediaries, Internet Service Providers, cyber cafes, Government sectors, private sectors, teachers, students, parents and general public to be aware about effect of this dangerous threat to society.

There is a great need to develop infrastructure in the tune of new multimedia technology in every sphere including judiciary.

Mobile phone providers must not provide mobile service with camera facilities without proper security and identity of person. However they can make compulsory undertaking from purchasers and service users that they will be liable for their illegal use, abuse, misuse of devices and service.

Banning mobile phone within the premises of educational institutions is one firm way to prevent cyber pornography within institutions.

There is great need to impose more responsibilities on the Internet Service Providers and cyber cafes. They must use filter system, firewall software, regular virus scanning system and verify all detail identifications of users i.e. with photo, address, date and time of use of particular computer by particular user and the like. More so, Internet Service Providers must have filter process and firewall to prevent cyber pornography.

Basic need is awareness about the result of this dangerous crime and also punishment. Even while any person uses the computer device, wireless or mobile phone for cyber pornography, after use he must delete those materials if he wishes to sell that mobile phone set to others. But those materials can be restored by using proper software. Therefore, proposed buyers and purchasers must keep in mind that those all deleted materials can be revived by using special gadgets like a memory card reader i.e., 3.8 software and therefore, they must verify accordingly. These possibilities are high in case of camera phone which has retrieval or reader facilities.

When we receive gifts from any one, we must check it whether it is bearing any spy camera or web camera through which criminals can watch our every second's activities and violate our right to privacy. For example, Any Time Monitoring (ATM) units with independent battery or GSM-enabled camera can transmit pornographic photos to the cell phone or computer.

Even when we are at our home we are not safe as was shown in film 'Chhoti se love story' where heroine was tapped by a boy from other building through a binocular.

From camera, the pornographic materials can be downloaded in a computer or mobile phone and then it can be published and transmitted through internet, email from computer to computer, computer to cell phone, cell phone to cell phone or cell phone to computer thus around the world.

Hackers, also crack down the websites and post their pornographic materials. Therefore, hackers' activities are to be curbed by law and awareness.

❖ Young net users must keep in mind that they must not disclose their personal identification in a chat room or face-to-face meeting programs without their parents consent.

Young users are very much interested to download objectionable materials and access those materials. Therefore cyber cafes as well as parents at home must keep a watch while children are using computer. They should not use it privately. It is again the prime duty of parents to be aware of them of those activities; so that they can develop their prudence to control passion for those harmful materials.

❖ Cyber cafe owners must take initiatives by monitoring whether any one especially young person is viewing pornographic websites so that they can be prevented and controlled.

❖ Cyber cafes must help police by providing every facility they require to control this crime.

In collaboration with the All India Association of Industries (AIAI), Mumbai police had taken initiatives for the Cyber Safety Week with the aim to spread awareness among the people so that they should know about such crimes and punishment. Other law enforcing agencies, Non-Governmental Organization's and Institutions must undertake such types of programs.

Parents can prevent this crime by monitoring their children whether they are spending more time in net during night or when alone? If so whether it was pornographic materials they were looking for? Whether they are receiving e-mails, calls, gifts from unknown person? Whether they have changed the scene frequently? Whether they are not attentive in family affairs? They may require counselling by psychologists.

One can easily monitor whether a person have used or is using pornographic website or stored materials through 'history' folder and Temporary Internet Files'. Therefore it is a way to control cyber pornography.

Everyone who finds that he or she became victim of cyber pornography or apprehended of this danger must without any fail immediately inform and lodge a complaint to police.

Cyber forensics has to be very active to detect, prevent and control cyber pornography.

There is need to adopt uniform law worldwide because this is not only a national problem but also an international problem. Therefore, there is a need to adopt specific laws on jurisdiction and international co-operation following European Convention 2001.

Cyber cafes, Internet Service Providers (ISP's) and parents must use filter software, timer clock of internet protocol etc and firewall to prevent minors from viewing and using objectionable websites and images. Cyber cafes and ISPs must demand photo identity cards to identify every user and to help investigations. They must investigate and detect machine, mobile phones etc after every use by the minors.

E-mail is a way of speedy communication, but it is being misused by cyber-criminals. It is because they know that detection and identification are not easy task here. Therefore, new technology users should adopt high standard of security and firewall.

Mobile phone with camera is an evil in our contemporary society. Here strict control is not possible because it is widely used. But there is a need to impose restrictions on it, i.e., identity cards, security measures, undertaking not to misuse it etc

Law enforcing machinery must be well equipped to investigate the matter and even they must be empowered to tap source of information and thereby deface websites. They must do so subject to right to privacy and national security.

In India we need to establish Special Cyber Crime Investigation Cell to investigate with well-equipped technology such as firewall, filter software.

There is great need of uniform information technology security standard world-wide. Net-users must have full knowledge about new technologies. All must be aware that ignorance of Law is not an excuse.

"When a man is denied the right to live the life he believes in, he has no choice but to become an outlaw."

To achieve the above objectives, we need to spread awareness among the public about the legal effect of misuse of new technology, cyber-crimes and self-protecting methods to prevent and control misuse of new technology.

Any person who wishes to protect their right to privacy in the cyberspace should adopt encryption process. Encryption process is a tool to Cyber Crime and protection of privacy in cyberspace. This is a process of self-protection or self-defence. There are two main key systems in encryption process, these are (i) public key and (ii) private key. When any one writes messages with encryption technique, such encryption turns that message into gibberish so that specific person to whom any one wishes to disclose or transfer his private information, that particular person only can access and read the said information by using proper key of the key pair. For example: X wishes to send confidential information with encryption through electronic mail to Z. X is confident that only Z can read the message and in it there is no likelihood of harm to these information. Here, X has to know the public key of Z. Then X will encrypt his message with Z's public key and a program called PGP. Then only Z can access the message by using process of decryption, sent by X to Z, by using his private key and hash function.

However, this method has a potential of being abused by the criminals. On the other hand, if net users, Government, institutions and organizations use this process then it will prevent and control Cyber Crimes such as unauthorized access, denial of service attack, attack on Government' information, attack on privacy, secrecy and confidential information. It will reduce abuse and misuse of Information Technology.

The Information Technology Act is also inadequate to apply in SMS cases where the Indian Penal Code I860 is not applicable in totality in the field of electronic messaging. It is also very difficult to control MMS clip because it is difficult to store these at the end of service. Therefore, service providers became vulnerable to check and control these. And the cell phone users do not have enough privacy protection system to prevent MMS clip. However, we can adopt the same process South Korea implemented in July 2004, making cell phone manufacturer mandatory to install a beep audible within a radius of 10 feet before using the camera mobile phone.

There was massive sale of MMS 'Video Clip' of two Delhi Public School, R.K. Puram student in Delhi Palika Bazaar, Nehru Place, Connaught Place markets for Rs. 50 to Rs. 250 even more. This was the scenario all over India and around the World through World Wide Web. The boy and girl were expelled from their school. Bazze.com's CEO Avnish Bajaj was arrested in spite of his assistance for investigation and co-operation to the police; it shows Indian police is very particular in duty and protecting society. But prison jurisprudence has to change in this regards e.g., person like Avnish Bajaj who is a respected personality in the Information Technology Industry was arrested by the police and lodged in the Tihar jail with other 70 prisoners charged from pick pocket to murder. There must be a reasonable classification in jail for the same. Though, jail or prison must not be like State's guest house. It is also not expected that such persons must be set free. In this regards. 67 must be specific when internet service providers will be liable and the extent of their liability.

Another exemplary step has been taken by Delhi Government by banning the use of mobile phone within any educational institutions Governmental as well as non-governmental. Recently the University of Calcutta, the Vishwa Bharati University, the University of Bardwan etc are also thinking for such banning.

The Communication Convergence Bill 2000 is lapsed after the incidents of MMS clip case be it Delhi Public School, Delhi Bal Bharti School where a student posted pornographic pictures of his classmate girls and teachers as a revenge of teasing for his vulnerability. Again April 2005 incidents of Delhi Amity Management School's girl students MMS clip came to light. MMS clip of APJ School's female student in North Delhi were showing dropping cloth for two minutes as her boyfriend may appreciate it. This MMS clips are in great demand by teenagers and mobile phone users. In market, second hand and even first hand mobile phones are selling with MMS clips as extra facilities.

The situation can be curbed by the law enforcement agencies, more so police by regular track, search, seizure process, frequent visit of those suspected places to nip in the bud. With this, people of India must contribute in the process of prevention and control of cyber pornography.

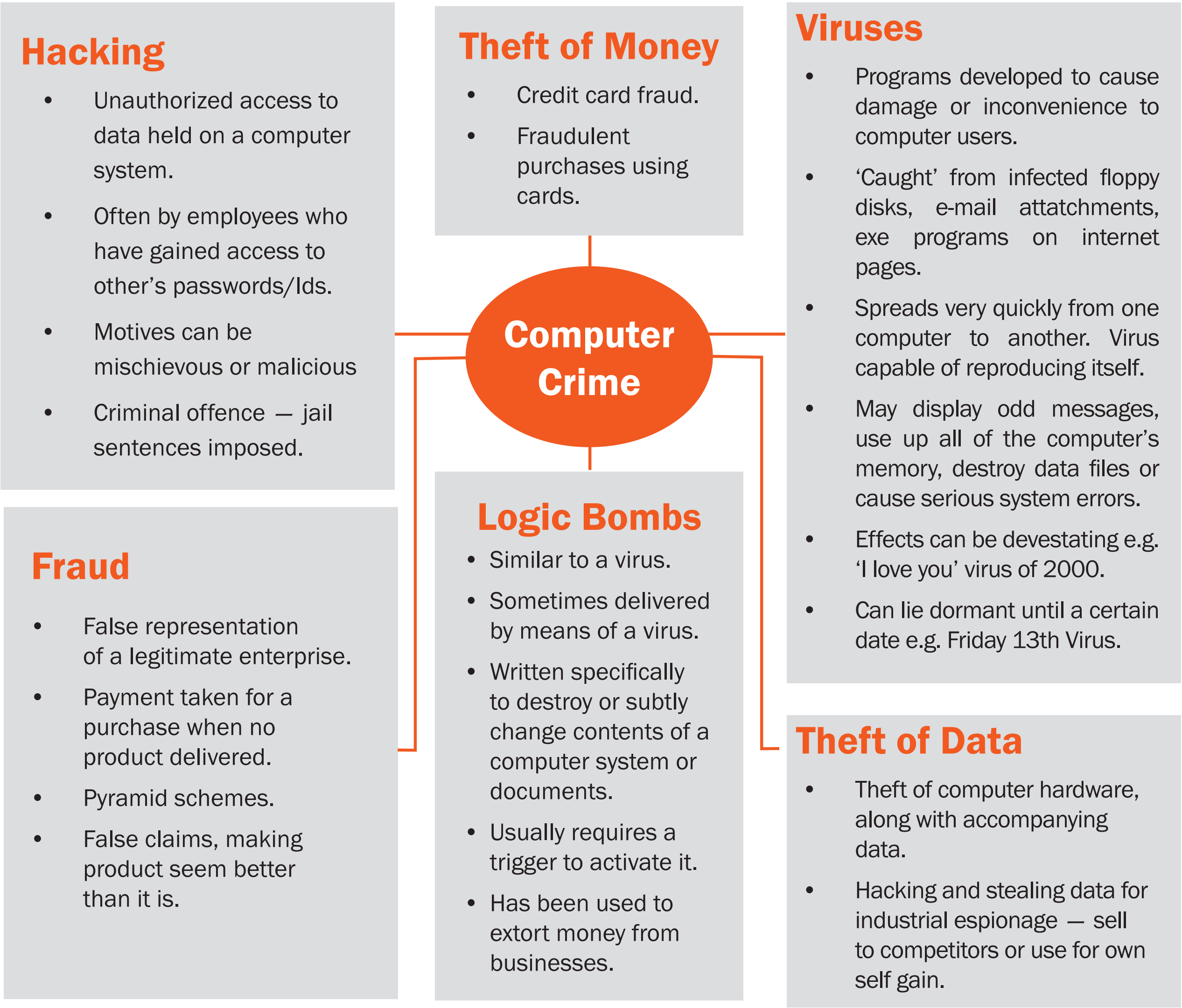
अध्याय 4
Chapter 4
Cyber Crime

Notes :

4.1 General:

Crime Overview Computer Crime:

Computer crime: which is also variously referred to as cyber-crime, e-crime, high-tech crime, and electronic crime — can include many different types of offenses. If a computer or a network is the source, target, tool or place of the crime, it is considered as a type of computer crime. Other crimes that can be facilitated by a computer crime are fraud, theft, blackmail, forgery and embezzlement.



Computer Crime

Hacking

- Unauthorized access to data held on a computer system.
- Often by employees who have gained access to other's passwords/Ids.
- Motives can be mischievous or malicious
- Criminal offence — jail sentences imposed.

Theft of Money

- Credit card fraud.
- Fraudulent purchases using cards.

Viruses

- Programs developed to cause damage or inconvenience to computer users.
- 'Caught' from infected floppy disks, e-mail attatchments, exe programs on internet pages.
- Spreads very quickly from one computer to another. Virus capable of reproducing itself.
- May display odd messages, use up all of the computer's memory, destroy data files or cause serious system errors.
- Effects can be devestating e.g. 'I love you' virus of 2000.
- Can lie dormant until a certain date e.g. Friday 13th Virus.

Fraud

- False representation of a legitimate enterprise.
- Payment taken for a purchase when no product delivered.
- Pyramid schemes.
- False claims, making product seem better than it is.

Logic Bombs

- Similar to a virus.
- Sometimes delivered by means of a virus.
- Written specifically to destroy or subtly change contents of a computer system or documents.
- Usually requires a trigger to activate it.
- Has been used to extort money from businesses.

Theft of Data

- Theft of computer hardware, along with accompanying data.
- Hacking and stealing data for industrial espionage — sell to competitors or use for own self gain.

Fig. 4.1. Types of Computer Crime

Computer crimes are covered by both federal and state laws. Because of the nature of technology, including the use of the Internet, computer crimes often cross state lines and therefore involve federal laws and federal prosecution. They can be classified as two separate categories of crimes; one in which the target is the network or computer, and one in which crimes are executed or expedited by a computer. Due to the usage of the Internet for e-commerce, and the total dependence on technology of many businesses, computer crime is predicted to advance. As new technologies take hold, criminal elements will infiltrate the systems for their benefit.

4.2 Events — Chronology:

Ever since the Act came into being there were series of demands for bringing about changes that will make sure that the Act provided for curbing the menace of Cyber Crime, issues of data leakage and personal privacy also started making news. These demands for change were further strengthened by the BPO industry in India which had to produce credentials of data safety and privacy in India to bid for international projects which were being outsourced out of western countries. A major amendment was made to the Act with effect from 6 February 2003 consequent to the passage of a related legislation called Negotiable Instruments Amendment Act, 2002. The amendment to Negotiable Instruments Act, 2002 for the first time recognized a cheque in electronic form. These changes notwithstanding, Indian Government realizing the changing terrain of online interactions, formed an expert committee under Ministry of Information Technology to suggest amendments to Act to keep it relevant. Main reasons for looking into changes in the Act were,

a. subject-matter being Information Technology which has an accelerated, pace of development;

b. intensive approach employed in it as opposed to a general framework to regulate information technology.

The committee pointing out several lacunas in the enactment proposed amendments to it in the report it tendered to the ministry of information technology. The result was the Information Technology Amendment Bill, 2006 based on the report submitted by the expert committee.

During the same time, in order to provide for protection of data leakage and personal privacy a Personal Data Protection Bill was introduced in Rajya Sabha in 2006. This bill, however, remains to be passed. The Information Technology Act 2000 amendment Bill 2006 has since been passed by the Indian Parliament on December 23, 2008.

4.3 Meaning of Cyber Crimes:

Cyber Crimes are crimes committed in electronic mediums where *mens rea* is not a requirement. The Cambridge Dictionary defines Cyber Crimes as crimes committed with the use of computers or relate to computers especially through the internet.

The Cyber Crime is an unlawful act wherein computer is either a tool or a target or both.

Cyber Crime is a generic term, which refers to all criminal activities done using the medium of computers, internet cyberspace and the world wide. Cyber Crimes are crimes that occur in the digital place, which is the aggregation of the transaction space within each of the connected computers and the virtual spaces arising out of the connection. In short the Cyber Crimes can be defined as offences or contradictions under any law committed with the use of electronic documents.

4.4 What is Cyber Crime?

Cyber Crime is an amalgamation of two words: 'cyber' — related to internet or other electronic networks and 'crime' — a criminal activity. Literally, the word cyber according to Oxford Learners Dictionary means:

"Connected with electronic communication networks, especially the Internet."

The word cyber is generally misunderstood as the word only and wholly concerned with the web and internet however; it also includes other communication networks electronic networking devices e.g. cellular networks and devices, telephones and many other e-devices.

The word crime as defined by Merriam-Webster dictionary:

"An act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law Oxford dictionary also defines crime as: 'an act punishable by law´.

Cyber Crime contains all criminal offences, which are committed with the aid of communication devices in a network. This can be for example the Internet, the telephone line or the mobile network. It is also known as computer crime and is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy, Cyber Crime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. In his book named 'What is Cyber Crime?, the author Nagpal R. defined: "Unlawful acts wherein the computer is either a tool or target or both".

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, Cyber Crime was broken into two categories and defined thus:

a. Cyber Crime in a narrow sense (computer crime): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cyber Crime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network; including such crimes as illegal possession (and) offering or distributing information by means of a computer system or network.

Cyberspace is the most eminent place for E-commerce, entertainment, social networking, information and many more. But, due to the evil minded 'netizens' (a combo derived from net and citizens for the persons using internet) this technology is nowadays being manipulated to commit offences which we call Cyber Crime. Some of the examples of Cyber Crimes are hacking, spamming, stealing identities and privacy, fraud, viral and worm attacks, e-mail bombing, cyber torts, cyber terrorism, trafficking, pornography, etc These crimes in the cyberspace have been a pain in the head and hole in the pocket of other users since the early days. In the early centuries, only the developing countries and mostly the US had accepted computers and internet and were the early victims of the cyber villains. However, in the contemporary world, hardly a hamlet remains that had not been touched by Cyber Crime of one sort or another.

Cyber Crime is an evil having its origin in the growing dependence on computers in modern life. A simple yet sturdy definition of Cyber Crime would be "unlawful acts wherein the computer is either a tool or a target or both". Defining Cyber Crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many Cyber Crimes, such as e-mail spoofing, cyber defamation etc

FIRST RECORDED
Cyber Crime

- The first Cyber Crime ever recorded was In France during 1820.
- The person involved was Joseph-Marie Jacquard.
- He was a textile manufacturer, he made looms.
- He invented looms that can store designs.

4.5 Against Economy—Cyberspace, in Current World, has become the Place where Commerce and Money is Moving which is Very Luring for the Criminals:

The criminals armed with technological sophistication have found it much easier to carry their activities in cyber word. Some of these crimes are as follows :

4.5.1 Hacking:

The term 'computer hacking' traditionally describes the penetration of computer systems, which is not carried out with the aims of manipulation, sabotage, but for pleasure of overcoming the technical security measures. Hacking has now become a "basic offence" which is then used to commit acts of espionage, software piracy, sabotage, as well as computer fraud. Hacking is punishable under Sections 66 and 70 of Information Technology Act 2000 with punishment up to 10 years of imprisonment or ₹2 lakhs fine or both.

4.5.2 Malicious Programs:

Malicious programs such as Virus-Worms, Trojan Horses, Logic Bombs, Hoaxes etc intend to cause harm to its victims.

a) **Virus:** It is a program that searches out other program and infects them by embedding a copy of it in them "Section 13(c) of the Information Technology Act covers the area of introduction of viruses, etc and shall be liable to pay damages by way of compensation not exceeding ₹1 crore to the person so affected.

b) **Worms:** These are the programs that propagate itself over a network reproducing itself as it goes. Worm unlike virus does not require a medium to propagate itself and infect others.

c) **Trojan:** A Trojan horse program pretends to do one thing while actually doing something completely different. Trojans let a hacker access the victim's hard disk; and also perform many functions on his computer. In the past there have been many incidents, in India and abroad, where Trojans have been used to alter the information contained in hospital computers.

d) **Logic bombs:** Logic bombs, once detonated in a computer, makes the program to go into an infinite loop, crash the computer, delete data files, or some other damage to the computer or its data.

e) **Hoax:** It is false warning about existence of malicious program.

Spreading rate of Malware Samples in different domains is shown in fig.

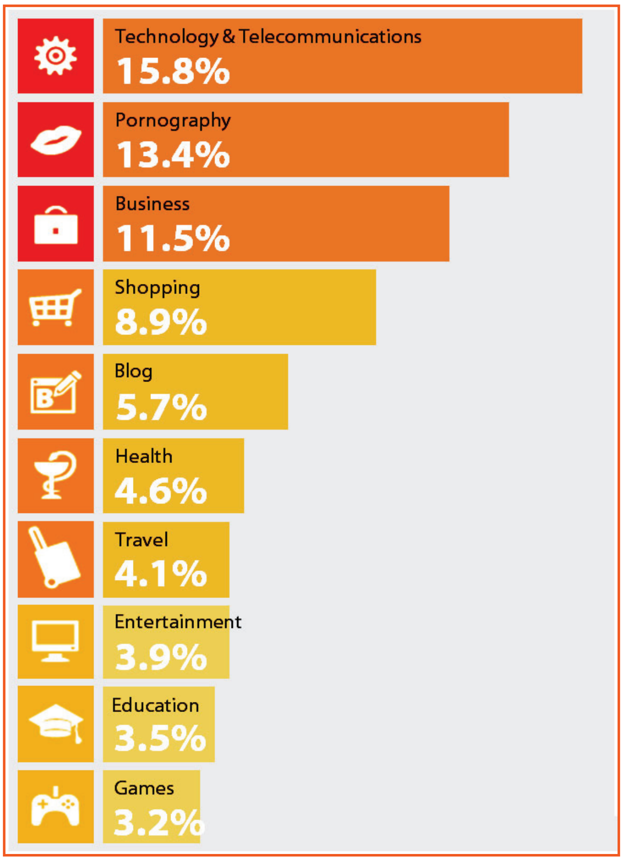


Fig. 4.2. Spreading rate of malware samples in different domains

4.5.3 Digital Forgery:

Digital technology facilitates perfect reproduction of documents. By using a computer, it is very easy to forge a document through printers and scanner by developing counterfeit currency, postal cards, revenue stamp, mark sheet, birth certificates etc Section 91 of Information Technology Act (read with second schedule) and amended provisions of IPC in relation to 'forgery' for the penal provisions of digital forgery.

4.5.4 Piracy and Infringement of Intellectual Property Rights:

Accessible, sufficient and adequately funded arrangements for the protection of rights are crucial in any worthwhile intellectual property system. There is no point in establishing a detailed and comprehensive system for protecting intellectual property rights and disseminating information concerning them. If it is not possible for the right-owners to enforce their rights effectively in a world where expanding technologies have facilitated infringement of protected rights to a hither to unprecedented extent. They must be able to take action against infringers in order to prevent further infringement and recover the losses incurred from any actual infringement. They must also be able to call on the state authorities to deal with counterfeits.

All intellectual property systems need to be underpinned by a strong judicial system for dealing with both civil and criminal offences, staffed by an adequate number of judges with suitable background and experience. Intellectual property disputes are in the main matters to be decided under civil law and the judicial system should make every effort to deal with them not only fairly but also expeditiously. Without a proper system for both enforcing rights and also enabling the grant of rights to others to be resisted, an intellectual property system will have no value. Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. Piracy and Infringement of Intellectual Property Rights are one of the most critical crimes committed in cyberspace. Section 2(o) of the Copyright Act, 1957 affords copyright protection in India wherein the term literary work' includes computer programs, tables and compilations including computer database and criminal proceedings that could be started under Sections 63–70 of the Act.

4.6 Cyber Warfare:

Cyber warfare is Internet-based conflict involving politically motivated attacks on information and information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems — among many other possibilities. The cyber warfare has gained so much favour among the military strategists that most of the Armies world over have dedicated cyber warfare teams for defensive as well as offensive operations. Defence planners around the world are investing substantially in information warfare — means of disrupting the information technology infrastructure of defence systems.

4.7 Computer Related Crimes:

Over the past 20 years the technology of electronic data processing — the computer — has come to play a dominant role in business and government. It would be difficult to conceive of a person whose life is not in some way affected by the computer, for virtually everyone who has a bank account, engages in any kind of credit transaction, or has dealings with the government or any large organization is touched by it in some way. The computer is now an indispensable tool for banking, corporate records and various activities of government.

The following diagram demonstrates many different ways Cyber Criminals can make money by hacking.

But the very features of the technology that make it such a boon to society also increase its susceptibility to abuse. The absence of tangible printed records of credit transactions is testimony to the efficiency of the computer, yet it leaves the auditor without the accustomed "paper trail" for verifying accounts. A computer need not be manipulated at any particular place, but can be operated from a distance using telecommunications facilities. This too can increase the potential for abuse, for now a thief need not be near the site of the crime but can, from the relative safety of a computer terminal, acquire assets reduced to electronic impulses.

Computer Related Crimes Covered under IPC and Special Laws:

Offence	Sections
Sending threatening messages by email	**Sec. 503, IPC**
Sending defamatory messages by email	**Sec. 499, IPC**
Forgery of electronic records	**Sec. 463, IPC**
Bogus websites, cyber frauds	**Sec. 420, IPC**
Email spoofing	**Sec. 463, IPC**
Web-Jacking	**Sec. 383, IPC**

E-Mail Abuse	**Sec. 500, IPC**
Online sale of Drugs	**NDPS Act**
Online sale of Arms	**Arms Act**

4.8 The Basic Problems Associated with Cyber Crimes:

One of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law anywhere in the world. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of Information Technology Act and amendments made to Indian Penal Code, problems associated with Cyber Crimes continue to persist.

1. Jurisdiction is the highly debatable issue as to the maintainability of any suits, which has been filed. Today with the growing arms of cyberspace the territorial boundaries seem to vanish. Thus the concept of territorial jurisdiction as envisaged under Section 16 of Cr PC and Section 2 of the IPC will have to give way to alternative method of dispute resolution.
2. Loss of evidence is a very common and expected problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.
3. Cyber Army: There is also an imperative need to build a high technology crime and investigation infrastructure, with highly technical staff at the other end.
4. A law regulating the cyber-space, which India has done.
5. Though Section 75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.
6. Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such case, which needs appreciation, is the PIL (Public Interest Litigation), which the Kerala High Court has accepted through an email.

'Perfect' is a relative term. Nothing in this world is perfect. The persons who legislate the laws and bye-laws also are not perfect. The laws therefore enacted by them cannot be perfect. The cyber law has emerged from the womb of globalization. It is at the threshold of development. In due course of exposure through varied and complicated issues it will grow to be a piece of its time legislation.

4.9 Legal Protection against Cyber Crime in India:

Cyber Crime cases have increased significantly in India. However, there is a general lack of awareness among public at large as well as police and judicial system regarding cyber law and Cyber Crimes.

As a result most of the Cyber Crimes are not reported at all. Even if some Cyber Crimes are reported, they are not investigated properly and this results in very few Cyber Crime convictions.

In most of the cases, lack of Cyber Crime conviction is the primary result of absence of proper legal assistance to prosecute Cyber Crimes. We have very few cyber law firms in India that are truly cyber law firms. Perry4Law is the best cyber law firm of India that is providing cyber law and other techno legal services.

In fact, the techno legal segment of Perry4Law known as Perry4Law's Techno Legal Base (PTLB) is managing the exclusive techno legal Cyber Crime investigation centre of India. The Cyber Crime investigation centre is playing a conclusive role in conducting Cyber Crime investigations in India and providing techno legal services to the victims of Cyber Crimes and cyber frauds.

With rapid digitalization of businesses and increasing cyber attacks. Organizations and Governments rightfully worry about the security of computer networks and infrastructures. A deeper and richer understanding of the principles and purposes; necessary and sufficient conditions for web attacks; and the patterns of origin and targets would help managers as well as national and international policy makers devise strategies to combat such crimes. The cyber laws of India are contained in the Information Technology Act 2000. The Act came into effect following the clearance of the Information Technology Bill, 2000 in May, 2000 by both the Houses of the Parliament. The Bill received the assent of the President of India in August, 2000 (Information Technology Act 2000). The Information Technology Act 2000 aims to provide the legal infrastructure for e-commerce in India. At this juncture, it is relevant to understand what the Information Technology Act 2000 offers and its various perspectives.

4.10 Various Online Frauds and Financial Crises:

During the recent financial crisis, no issue has aroused more passion than financial institution bailouts. The standard rationale for the bailouts has been one of the necessity and fear: federal regulatory agencies must have more authority in order to respond to the crisis, or else the public will face terrible consequences. But does this rationale hold up to close inspection?

The nation's federal financial regulators and the politicians claim to have saved the American economy. In truth they have done everything within their power to expand their own influence — often far out of view from the public and media. Instead of openly explaining their actions, the bailout agencies have attempted to prevent the public from reviewing their decision-making, often at tremendous cost to taxpayers.

Identity theft and frauds are crimes where someone wrongfully obtains and uses another's personal data in a way that involves fraud or deception for financial gain. To avoid these types of offences giving of personal details to others should be avoided.

Another category of money related crime is credit card fraud. Here again somebody's credit card may be wrongfully used for one's personal gain. This risk has grown multifold as people do purchase online through their credit cards. The websites offering product take all the details of the credit card and store information on the server. So anybody who can access the server can use the credit card details for financial gains.

Apart from this, financial frauds includes market manipulation scheme, issuance of false stock, online gambling, sale of illegal articles.

The word fraud has not been defined in the Indian Penal Code. However, Section 25 of IPC defines the word 'fraudulently' as, there can be no-fraud unless there is an intention to defraud. Wherever the words fraud, intent to defraud or fraudulently occur in the definition of a crime under the IPC, two elements at least are essential to the commission of that crime.

1. Deceit or an intention to deceive, and
2. Either actual injury or possible injury or an intent to expose some person to actual or possible injury.

Both are essential requisites of fraud i.e. deceit or intention to deceive and actual or possible injury to an individual are present in all such seams, intended to gain advantage at the risk of loss to others.

4.11 Cyber Crime Preventive Methods:

Computer is now emerging as a new crime tool. The growing menace from crimes committed against computers, or against information on computers, is commanding the attention of various nations. The phenomenal growth of computers and Internet services has engendered the problem of Cyber Crime proliferation on the account of investigation difficulties and lack of strong evidences. Further, existing laws and preventive measures are not effective to curb such crimes. This lack of legal protection calls for businesses and governments to adopt solid technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. This paper discusses ramifications of Cyber Crime including discussion on current and emerging forms of computer related illegalities and tools and techniques used in such crimes. In addition, some preventive measures are suggested that can be taken by corporate houses and law enforcement agencies including framing of new laws and subsequent issues that arise.

Computer crime is an expanding division of criminal activity. Also known as Cyber Crime, cases include intrusion/infiltration, financial and identity theft, espionage, and cyber warfare. Computer crime may also include child pornography and copyright infringements, as well as any other illegal activity that was performed with assistance of a computer.

Not only the law is for people but people are also for the law. Prevention is better than cure and so the common people must take some preventive measures to be out of the evil sight of Cyber Crimes. First comes the 'VIGILANCE.' Without knowing the enemy, one cannot combat it. Thus, people require to know and being vigilant about the cyberspace and the dark fissure of crimes committed there within. The netizens must be updated with the information regarding cyber worlds and the techniques to use them. Moreover, the authorities too should be dwelled with the knowledge regarding these spheres of internet so that they can manipulate the law to outcome the problems of cyberspace. Cyber insurance should also be done for the companies so that their loss may be compensated.

Thousands of Cyber Crimes plague the country every year. Yet, not a single Indian Insurance company offers a comprehensive anti-Cyber Crime policy for the corporate sector. "In India there are few takers for Cyber Crime insurance primarily because of the high cost vis-a-vis their exposure. These policies are of a high value and, on request from a few brokers, are customised for banks. We sell one or two policies a year," an HDFC Ergo official explained. The anti-virus software must be updated regularly and firewalls arid spywares must be installed in each and every computer systems. Information should not be provided to each and every sites blindly. One should only rely on the sites he/she trusts. An eye on the children by the parents could serve as an anti-pornography campaign.

This will be good both for the children as well as for parents to eradicate Cyber Crime. Backup must be kept for the important data so that viral contamination cannot chew up any important information. Another milestone in ensuring the safety and security of the people through advanced means of Information Technology was added with the launching of the Cyber Crime investigation cell by the Punjab Governor and Administrator, Union Territory, Chandigarh, Gen. (Retd.) S.F. Rodrigues, at an impressive function in police station. Set up by the Chandigarh Police with the participation of NASSCOM and Punjab Engineering College, Chandigarh this Cell will help in checking computer related crimes, such as unauthorized access to a computer, online banking fraud, "phishing", sale of illegal articles like wildlife products, drugs etc, pornography, online gambling, e-mail spoofing and cyber stalking.

New law should be organized which wholly deals with the evils of cyber-crime covering all the spheres of cyberspace and the officers must be appointed having valid qualification efficient fully in cyberspace and crimes in it. Following some of these ways, one can be in safe hands in the world of cyberspace and the Cyber Crimes can be prevented more efficiently.

4.12 Preventive Steps for Individuals:

4.12.1 Children:

Children should not give identifying information such as Name, Home address, School Name or Telephone Number in a chat room. They should not share photographs with anyone on the net without first checking or informing parents, guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a face-to-face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

4.12.2 Parents:

Parent should use content filtering software on PC to protect children from pornography, gambling, hate speech, drugs and alcohol.

There is also a software to establish time controls for use of limpets (for example blocking usage after a particulars time) and allowing parents to see which site their children have visited. Parents can use this software to keep track of the type of activities of children.

4.12.3 General Information:

Don't delete harmful communications (emails, chats etc). They will provide vital information about system and address of the person behind these:

- Try not to panic.
- If you feel any immediate physical danger contact your local police.
- Avoid getting into huge arguments online during chat and discussions with other users.
- Remember that all other Internet users are strangers; you do not know who you are chatting with. So be careful.
- Be extremely careful about how you share personal information about yourself online.
- Choose your chatting nickname carefully so as others.
- Do not share personal information in public space online; do not give it to strangers.
- Be extremely cautious about meeting online introduced person. If you choose to meet do so in a public place along with a friend.
- If an online situation becomes hostile, log off and if a situation places you in fear, contact the local police.
- Save all communications for evidence. Do not edit it in any way. Also, keep a record of your contacts and inform Law Enforcement Officials.

4.13 Preventive Steps for Organizations and Government:

Computer is now emerging as a new crime tool. The growing menace from crimes committed against computers, or against information on computers, is commanding the attention of various nations. The phenomenal growth of computers and Internet services has engendered the problem of Cyber Crime proliferation on the account of investigation difficulties and lack of strong evidences. Further, existing laws and preventive measures are not effective to curb such crimes. This lack of legal protection calls for businesses and governments to adopt solid technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. This paper discusses ramifications of Cyber Crime including discussion on current and emerging forms of computer related illegalities and tools and techniques used in such crimes. In addition, some preventive measures are suggested that can be taken by corporate houses and law enforcement agencies including framing of new laws and subsequent issues that arise.

Computer crime is an expanding division of criminal activity. Also known as Cyber Crime, cases include intrusion/infiltration, financial and identity theft, espionage, and cyber warfare. Computer crime may also include child pornography and copyright infringements, as well as any other illegal activity that was performed with the assistance of a computer.

*"Those who have wisdom have all: Fools with all have nothing."***- Thiruvalluvar**

4.13.1 Physical Security:

Overview:

If an intruder gets physical access to a computer, they can easily gain access to the information stored on the computer. Methods range from simply tucking the computer under their arm and walking off with it to collect the data at leisure, using a ´rescue disk´ or some other method of starting the computer with no passwords, removing the hard drive and starting it on their own computer, with full access to the information stored on the drive.

Most operating systems have some method of starting the computer with no passwords — this is intentional, because most organizations will lose or forget a critical password at some time. This can only be done when a person is physically present at the computer, however — the operating system designers rely on the user being aware of this fact, and securing the computer room. There are methods, in most operating systems, of disabling the 'no password' start — if you choose to implement them, be extremely careful and document the passwords well. But secure the copy of the passwords. Physical security is the most sensitive component, as prevention from Cyber Crime Computer network should be protected from the access of unauthorized persons.

4.13.2 Access Control:

Simply defined, the term ˝access control˝ describes any technique used to control passage into or out of any area. The standard lock that uses a brass key may be thought of as a simple form of an ˝access control system˝.

Over the years, access control systems have become more and more sophisticated. Today, the term ˝access control system˝ most often refers to a computer-based, electronic card access control system. The electronic card access control system uses a special "access card", rather than a brass key, to permit access into the secured area.

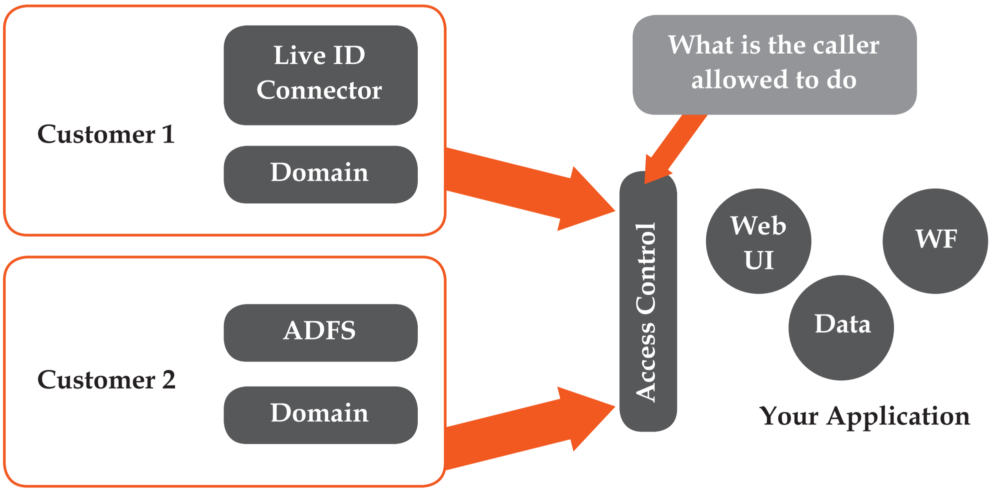


Fig. 4.3. Access Control

*Strength is life, weakness is death. Strength is felicity, life eternal, immortal. Weakness is constant strain and misery; weakness is death. - **Swami Vivekananda***

Access control systems are most commonly used to control entry into exterior doors of buildings. Access control systems may also be used to control access into certain areas located within the interior of buildings.

The purpose of an access control system is to provide quick, convenient access to those persons who are authorized, while at the same time, restricting access to unauthorized people.

Few employers allow all their employees to access all facilities every time. That's why more and more are using electronic access control to limit employees' access to their facilities. At a minimum, an electronic access control system can be used to allow only employees into a building after hours, and provide excellent documentation of when and where employees enter and exit. Access control is the only technology that proactively attempts to keep unauthorized individuals out of a building or areas within a facility, and is a perfect complement to video surveillance, burglar and fire systems in a comprehensive security solution proposal.

Access Control system is generally implemented using firewalls, which provide a Centralized point from where to permit or allow access. Firewalls allow only authorized communications between the internal and external network.

4.13.3 Password:

A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. Typically, users of a multiuser or securely protected single-user system claim a unique name (often called a user ID) that can be generally known. In order to verify that someone entering that user ID really is that person, a second identification, the password, known only to that person and to the system itself, is entered by the user. A password is typically somewhere between 4 and 16 characters, depending on how the computer system is set up. When a password is entered, the computer system is careful not to display the characters on the display screen, in case others might see it.

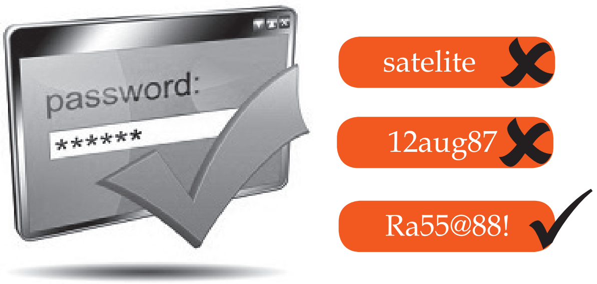


Fig. 4.4. Password Examples

Proof of identity is an essential component to identify intruders. The use of passwords in the most common security for network system includes servers, routers and firewalls. Mostly all the systems are programd to ask for username and password for access to computer system. This provides the verification of user. Password should be changed with regular interval of time and it should be alpha numeric and should be difficult to judge.

4.13.4 Finding the Holes in Network:

Exploiters on the Internet have caused billions of dollars in damages. These exploiters are intelligent cyber terrorists, criminals and hackers who have a plethora of tools available in their war chests ranging from spyware, root kits, Trojans, viruses, worms, bots, and zombies to various other blended threats.

Exploits can be grown and harvested the same day a security hole is announced — in so-called "zero-day attacks" — so they are getting much harder to stop. Open source malware code, freely available on the Internet, is enabling this phenomenon and cannot be reversed. Although the number and types of exploits "in the wild" continues to rise exponentially, there are fewer than a dozen core methodologies used for their execution and proliferation. Most exploits can be removed, but some exist indefinitely and can only be destroyed or removed by loss of data — you've probably heard of these "root kits." Most exploits will re-infect a host if a security hole, also known as the Common Vulnerability and Exposure (CVE), is not removed.

System managers should track down the holes before the intruders do. Many networking product manufactures are not particularly aware with the information about security holes in their products. So organization should work hard to discover security holes, bugs and weaknesses and report their findings as they are confirmed.

4.13.5 Using Network Scanning Programs:

Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweeps and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer. Another scanning method, inverse mapping, returns information about what IP addresses do not map to live hosts; this enables an attacker to make assumptions about viable addresses.

Scanning is one of the three components of intelligence gathering for an attacker. In the foot printing phase, the attacker creates a profile of the target organization, with information such as its domain name system (DNS) and e-mail servers, and its IP address range. Most of this information is available online. In the scanning phase, the attacker finds information about the specific IP addresses that can be accessed over the Internet, their operating systems, the system architecture, and the services running on each computer. In the enumeration phase, the attacker gathers information such as network user and group names, routing tables, and Simple Network Management Protocol (SNMP) data.

There is a security administration's tool called UNIX, which is freely available on Internet. This utility scans and gathers information about any host on a network, regardless of which operating system or services the hosts were running. It checks the known vulnerabilities including bugs, security weakness, inadequate password protection and so on. There is another product available called COPS (Computer Oracle and Password System). It scans for poor passwords, dangerous file permissions, and dates of key files compared to dates of CERT security advisories.

4.13.6 Using Intrusion Alert Programs:

This tool is designed to facilitate the interactive analysis of alerts reported by Intrusion Detection System (IDS). It was started as a prototype system and was developed to validate who method to correlate intrusion alerts based on the prerequisites and consequences of known attacks (See our paper in CCS '02). Now it has been serving as a platform to test and validate our techniques for intrusion analysis. who would also like to transform our techniques into a

*The whole secret of existence is to have no fear. Never fear what will become of you, depend on no one. Only the moment you reject all help are you free. - **Swami Vivekananda*** practical tool that helps intrusion analysis in real-world applications.

TIAA is written in Java. The current version is an offline tool interacting with DBMS.

As it is important to identify and close existing security holes, you also need to put some watch dogs into service. There are some intrusion programs, which identify suspicious activity and report so that necessary action is taken. They need to be operating constantly so that all unusual behaviour on network is caught immediately.

4.13.7 Using Encryption:

Encryption is a process which is applied to text messages or other important data, and alters it to make it humanly unreadable except by someone who knows how to decrypt it. The complexity of the algorithms used means that a strongly encrypted message might require thousands of years of processing by very fast computers to break the encryption.

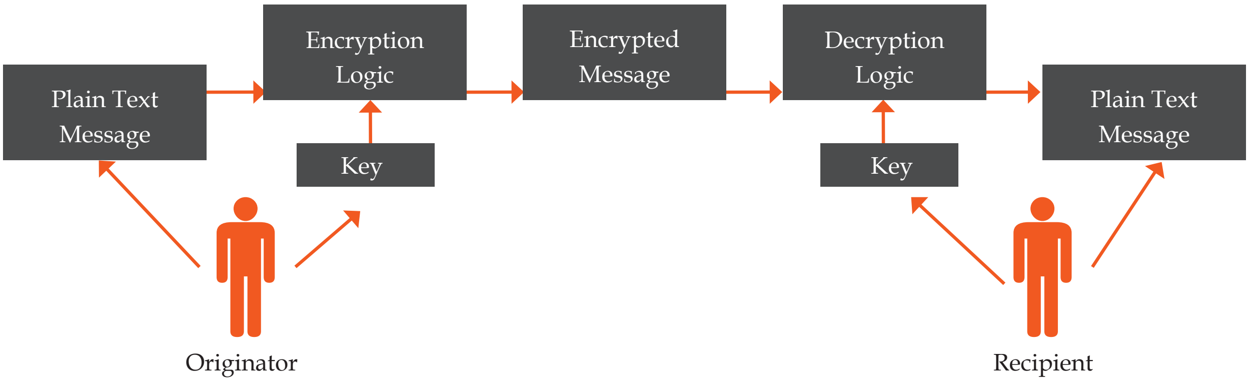


Fig. 4.5. Symmetric Encryption

The most popular use of encryption is for securing web servers that are accessed by the https protocol not http so that data such as credit cards can be sent safely over the internet. Encryption is the conversion of data into a form, called a cipher text, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher — that is, the harder it is for unauthorized people to break it — the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

Encryption is able to transform data into a form that makes it almost impossible to read it without the right key. This key is used to allow controlled access to the information to selected people. The information can be passed on to anyone but only the people with the right key are able to see the information. Encryption allows sending confidential documents by E-mail or save confidential information on laptop computers without having to fear that if someone steals it the data will become public. With the right encryption/decryption software installed, it will hook up to mail program and encrypt/decrypt messages automatically without user interaction.

4.14 Problems Related with Cyber Crime:

4.14.1 Jurisdiction:

Power or right of a legal or political agency to exercise its authority over a person, subject matter, or territory. Jurisdiction over a person relates to the authority to try him or her as a defendant. Jurisdiction over a subject matter relates to authority derived from the country's constitution or laws to consider a particular case. Jurisdiction over a territory relates to the geographic area over which a court has the authority to decide cases. Concurrent jurisdiction exist where two courts have simultaneous responsibility for the same case.

Cyber attack have benefited from jurisdictional arbitrage. Because of the sophistication and newness, jurisdictional arbitrage is higher for Cyber Crimes compared to other conventional crimes. Only the US and the UK have laws that come even close to adequate in defining Cyber Crimes and levelling penalties. The lack of a strong rule of law is associated with origination of more cyber attacks. A strong rule of law is characterised by effective punishment of transgressors and regulatory sanctions for defectors and thus enhances the ability to successfully litigate fraudulent online dealings. There are international differences in terms of laws to minimise vulnerability to cyber attacks.

Organised Cyber Crimes are often initiated from countries that have few or no laws directed against Cyber Crimes and little capacity to enforce existing laws. For instance, when a Philippino hacker launched the “Love Letter” virus in 2000, estimated loss of damage in the US was in the range of $4–15 billion. But the US Government could not do anything to prosecute the hacker or to recover the damages because at that time the Philippines had not enacted laws that prohibited such crimes. Although many countries in world have enacted Cyber Crime.

A nation’s laws also determine what is considered to be a Cyber Crime. National laws also facilitate or restrict law enforcement agencies ability to act on potential ingredients related to Cyber Crimes. In the US, for instance, the FBI considered militant Islamist websites lawful as the First Amendment permits even the most hateful Internet speech, as long as they don’t directly incite violence or raise money. On the contrary, in Singapore in the Cyber conflict with the Think Centre (Asia), an NGO, the State authorities reportedly employed surveillance and intimidation. There are reports that the Government of Singapore actively scans and monitors e-mails and there are instances of breaking into a number of computers used by various groups and individuals.

Law enforcement agencies responses also differ across types of Cyber Crimes. Experts argue that law enforcement officials in some countries don’t take major actions against hackers attacking international websites and are more interested in protecting national security.

4.14.2 Motivation:

Internal and external factors stimulate desire and energy in people to be continually interested and committed to a job, role or subject, or to make an effort to attain a goal.

Motivation results from the interaction of both conscious and unconscious factors such as the (1) intensity of desire or need, (2) incentive or reward value of the goal, and (3) expectations of the individual and of his or her peers. These factors are the reasons one has for behaving in a certain way. An example is a student who spends extra time studying for a test because he or she wants a better grade in the class.

Given the diversity of computer related crimes, it is not surprising that the various types of behaviour discussed above flow from a wide range of motives. Some of these are as old as human society, including greed, lust, revenge and curiosity. Revenge in the modern era can also entail an ideological dimension. Of considerable significance, if not unique to computer related crime, is the intellectual challenge of defeating a complex system. The motivation for the hackers and crackers could be stealing information or other assets, or merely an act of power wherein he feels powerful in being able to break in a system representing big business or Governmental organization.

4.14.3 Opportunities:

Definition:

Exploitable set of circumstances with uncertain outcome, requiring commitment of resources and involving exposure to risk.

Examples of Opportunity:

1. You'll have an opportunity to ask questions after the presentation.
2. When the opportunity came for her to prove that she could do the job, she was ready.
3. I had the rare opportunity of speaking to the president.
4. Studying abroad provides a great opportunity to learn a foreign language.
5. There are fewer job opportunities this year for graduates.
6. I would like to take this opportunity to thank everyone who helped me with this book.

The exponential growth in connectivity of computing and communications creates parallel opportunities for prospective victims. As the internet becomes increasingly a medium of commerce, it will become increasingly a medium of fraud. There are many technologies which reduce the opportunity to commit computer related crime such as technologies of authentication, from basic passwords, to various biometric devices such as finger print or voice recognition technology, and retinal imaging, which greatly enhance the difficulty of obtaining unauthorized access to information systems. Virus detectors can identity and block malicious computer code; blocking and filtering programs can screen out unwanted content. A rich variety of commercial software now exist with which to block access to certain sites.

4.14.4 Guardians:

Absence of capable guardianship is also a factor Cyber Crime. Guardianship against Cyber Crime involves preventive efforts on the part of prospective victims, contributions by members of the general public or commercial third parties, as well as the activities of law enforcement agencies. Indeed, it is often only when private efforts at crime prevention fail that the criminal process is mobilised. Capable guardianship has evolved over human history, from feudialism, to the rise of the state and the proliferation of public institutions of social control, to the post-modern era in which employees of private security services vastly out number sworn police officers in many industrial democracies. The basic tenets of the opportunity theory are that the level of crime is determined by the availability of suitable targets, the presence of motivated offenders and the absence of capable guardians.

4.14.5 Enforcement:

In present times, even where the crimes get reported, the prosecution rate is not very high as per worldwide trends available. The criminal justice administration systems are not equipped to deal with the highly technological crimes committed in cyber world. The traditional laws, procedures and the systems are unable to appreciate the nature of crime investigation and evidence in cyberspace for want of necessary technical knowledge. The need for enhancing the understanding about peculiarities of Cyber Crimes and cyber-evidences, by judicial officers. It is the judiciary who has the final word on any criminal prosecution and unless the awareness level among them is built up to meet the challenge of increasing Cyber Crimes, the rate of successful prosecutions will still be less. So to deter prospective offenders from undertaking any crime in cyberspace, the judicial understanding about cyber issues need to be enhanced.

4.15 Indian Case Studies:

CASE STUDY *36: NASSCOM v. Ajay Sood and others:* In a landmark judgment in the case of National Association of software and Service Companies v. Ajay Sood & others, delivered in March 05, the Delhi High Court declared ‘phishing’ on the internet to be an illegal act, entailing an injunction and recovery of damages.

Elaborating on the concept of ‘phishing’, in order to lay down a precedent in India, the Court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party’s advantage. Court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The Delhi High Court stated that even though there is no specific legislation in India to penalise phishing, it held phishing to be an illegal act by defining it under Indian law as “a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused.” The Court held the act of phishing as passing off and tarnishing the plaintiff’s image.

The plaintiff in this case was the National Association of Software and Service Companies (NASSCOM), India’s premier software association.

The defendants were operating a placement agency involved in headhunting and recruitment. In order to obtain personal data, which they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of NASSCOM. The High Court recognized the trademark rights of the plaintiff and passed an *ex parte ad interim* injunction restraining the defendants from using the trade name or any other name deceptively similar to NASSCOM. The Court further restrained the defendants from holding themselves out as being associates or a part of NASSCOM.

The Court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the Court. The offending e-mails were then downloaded from the hard disks and presented as evidence in Court.

During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs. 1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The Court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones. It brings the act of "phishing" into the ambit of Indian laws even in the absence of specific legislation. It clears the misconception that there is no "damages culture" in India for violation of IP rights. This case reaffirmed IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and sent a strong message to IP owners that they can do business in India without sacrificing their IP rights.

CASE STUDY ▷ ***37: Bazee.com Case:*** The CEO of bazee.com was arrested on December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the Cyber Crime cases and a lot of education is required on these things.

CASE STUDY ▷ ***38: The Bank NSP Case:*** The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many e-mails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients.

English is necessary as at present original works of science are in English. I believe that in two decades times original works of science will start coming out in our languages. Then we can move over like the Japanese. - ***Dr. A.P.J. Abdul Kalam***

She used the bank's computer to do this. The boy's company lost a large number of clients and took the bank to Court. The bank was held liable for the emails sent using the bank's system.

Case Study ***39: SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra:*** In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails and passed an important *ex parte* injunction.

In this case, the defendant Jogesh Kwatra being an employee of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R.K. Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.

On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the acts of the defenant in sending the emails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employee could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.

After hearing detailed arguments of counsel for plaintiff, Hon'ble Judge of the Delhi High Court passed an *ex parte ad interim* injunction observing that a *prima facie* case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an *ex parte* injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

Case Study ***40: Parliament Attack Case:*** Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop seized from the two terrorists, who were gunned down when Parliament was under siege on December 13, 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents.

Truth does not pay homage to any society, ancient or modern. Society has to pay homage to Truth or die.
- Swami Vivekananda

The laptop contained several evidences that confirmed the two terrorists' motives, the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal.

The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

CASE STUDY ▸ ***41: Pune Citibank Mphasis Call Centre Fraud :*** US $3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India. It is a serious matter and we cannot ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centres in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering.

The call centre employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber cafe and accessed the Citibank accounts of the customers.

All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call centre and has frozen the accounts where the money was transferred.

There is a need for a strict background check of the call centre executives. However, best of background checks cannot eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history. Customer education is very important so customers do not get taken for a ride. Most banks are guilty of not doing this."

CASE STUDY ▸ ***42: Andhra Pradesh Tax Case:*** Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person.

The owner of a plastics firm was arrested and Rs. 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers, it revealed that all of them were made after the raids were conducted. It later revealed

*If the deaf are to hear, the sound has to be very loud. When we dropped the bomb, it was not our intention to kill anybody. We have bombed the British Government. The British must quit India and make her free. - **Shahid Bhaghat Singh*** that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

CASE STUDY *43: Sony.Sambandh.com Case:* Indian saw its first Cyber Crime conviction recently. It all began after a complaint was filed by Sony India Private Ltd., which runs a website called www.sony.sambandh.com, targeting Non-Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Sections 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless head phone.

In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The Court convicted Arif Azim under Sections 418, 419 and 420 of the Indian Penal Code — this being the first time that a Cyber Crime has been convicted.

The Court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The Court therefore released the accused on probation for one year.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a Cyber Crime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of Cyber Crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

CASE STUDY *44: Infinity e-search BPO Case:* The Gurgaon BPO fraud has created an embarrassing situation for Infinity e-Search, the company in which Mr. Karan Bahree was employed."

A British newspaper had reported that one of its undercover reporters had purchased personal information of 1,000 British customers from an Indian call-centre employee. However, the employee of Infinity e-Search, a New Delhi-based web designing company, who was reportedly involved in the case has denied any wrongdoing. The company has also said that it had nothing to do with the incident.

In the instant case the journalist used an intermediary, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data is itself not substantiated by the journalist.

In this sort of a situation we can only say that the journalist has used "Bribery" to induce a "Out of normal behaviour" of an employee. This is not observation of a fact but creating a factual incident by intervention. Investigation is still on in this matter.

4.16 Types of Cyber Crime:

Cyber Crime IS AN EVIL HAVING ITS ORIGIN IN THE GROWING DEPENDENCE ON COMPUTERS IN MODERN LIFE.

"A simple yet sturdy definition of Cyber Crime would be unlawful acts wherein the computer is either a tool or a target or both". Defining Cyber Crimes, as "acts that are punishable by the information Technology Act" would be unsuitable as the Indian Penal Code also covers many Cyber Crimes, such as e-mail spoofing, cyber defamation, etc

1. ***Cyber Crime in a narrow sense (computer crime):*** Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.
2. ***Cyber Crime in a broader sense (computer-related crime):*** Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Cyber Crime refers to all activities done with criminal intent in cyberspace. These fall into three slots.

- Those against persons.
- Against Business and Non-business organizations.
- Crime targeting the government.

4.16.1 Financial Claims:

This would include cheating, credit card frauds, money laundering etc

4.16.2 Cyber Pornography:

This would include pornographic websites; pornographic magazines produced using computer and the Internet (to download and transmit pornographic pictures, photos, writing etc)

4.16.3 Sale of Illegal Articles:

This would include sale of narcotics, weapons and wildlife etc, by posting information on websites, bulletin boards or simply by using e-mail communications.

4.16.4 Online Gambling:

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

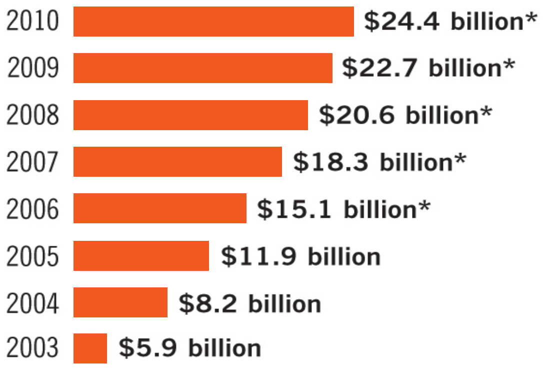


Fig. 4.6. Global Online Gambing Revenue

4.16.5 Intellectual Property Crimes:

These include software piracy, copyright infringement, trademarks violations etc

4.16.6 E-mail Spoofing:

A spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-mail forging.

4.16.7 Forgery:

Counterfeit currency notes, postage and revenue stamps, mark sheets etc, can be forged using sophisticated computers, printers and scanner.

4.16.8 Cyber Defamation:

This occurs when defamation takes place with the help of computers and or the Internet e.g. someone published defamatory matter about someone on a websites or sends e-mail containing defamatory information to all of that person's friends.

4.16.9 Cyber Stalking:

Cyber stalking involves following a person's movements across the internet by posting messages on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim.

Cyber Stalking

- 75 to 80% of stalkers are men stalking women
- Most Victims are women
- Most Stalkers are men

4.16.10 Unauthorized Access to Computer System or Network:

This activity is commonly referred to as hacking. The Indian Law has however given a different connotation to the term hacking.

"Every action that helps us manifest our divine nature more and more is good; every action that retards it is evil."
- Swami Vivekananda

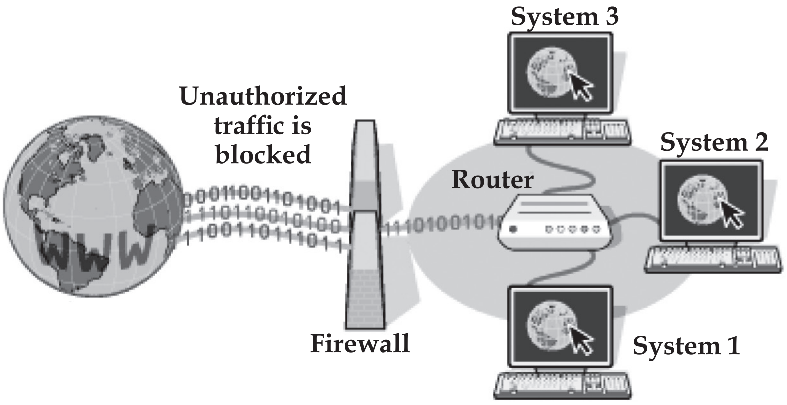


Fig. 4.7. Unauthorized access to computer system or network

4.16.11 Theft of Information Contained in Electronic Form:

This includes information stored in computer hard disks, removable storage media etc

4.16.12 E-mail Bombing:

Email bombing refers to sending a large amount of e-mails to the victim resulting in the victims' e-mail account or mail servers.

4.16.13 Data Diddling:

This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

4.16.14 Salami Attacks:

Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer.

4.16.15 Denial of Service:

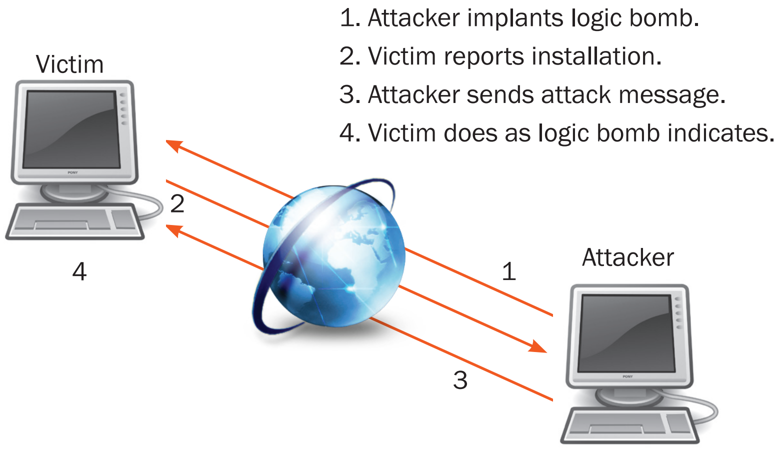
This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

4.16.16 Virus / Worm:

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to.

4.16.17 Logic Bombs:

These are dependent programs. This implies that these programs are created to do something only when a certain event occurs, e.g. some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date.



1. Attacker implants logic bomb.
2. Victim reports installation.
3. Attacker sends attack message.
4. Victim does as logic bomb indicates.

Fig. 4.8. Logic Bombs

4.16.18 Trojan Horse:

A Trojan as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

4.16.19 Internet Time Theft:

This connotes the usage by unauthorized persons of the Internet hours paid for by another person.

4.16.20 Physically Damaging a Computer System:

This crime is committed by physically damaging a computer or its peripherals.

4.17 Threat Perceptions:

Definition:

Threat perception is defined as a deep sense of vulnerability that is assumed to be negative, likely to result in loss, and largely out of one's control.

Threat perception is commonly viewed as a requirement to change organizational inertia.

UK has the largest number of infected computers in the world followed by the US and China. Financial attacks are 16 events per 1000, the highest among all kinds of attacks. The US is the leading source country for attacks but this has declined. China is second and Germany is third. It is hard to determine where the attack came from originally. The number of viruses and worm variants rose sharply to 7,360 that is a 64% increase over the previous reporting period and a 332% increase over the previous year. There are 17,500 variants of Win. 3 viruses. Threats to confidential information are on the rise with 54% of the top 50 reporting malicious code with the potential to expose such information, Phishing messages grew to 4.5 million from 1 million between July and December 2004.

4.18 Tools Used for Cyber Crime:

Botnets are becoming a major tool for Cyber Crime, partly because they can be designed to very effectively disrupt targeted computer systems in different ways, and because a malicious user, without possessing strong technical skills, can initiate these disruptive effects in cyberspace by simply renting botnet services from a cybercriminal botnets, or "Bot Networks", are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code. Botnets have been described as the "Swiss Army knives of the underground economy" because they are so versatile.

Botnet code was originally distributed as infected email attachments, but as users have grown more cautious, Cyber criminals have turned to other methods. When users click to view a spam message, botnet code can be secretly installed on the users' PC A website may be unknowingly infected with malicious code in the form of an ordinary looking advertisement banner, or may include a link to an infected website. Clicking on any of these may install botnet code. Or, botnet code can be silently uploaded, even if the user takes no action while viewing the website, merely through some un-patched vulnerability that may exist in the browser. Firewalls and anti-virus software do not necessarily inspect all data that is downloaded through browsers. Some bot software can even disable anti-virus security before infecting the PC. Once a PC has been infected, the malicious software establishes a secret communications link to a remote "botmaster" in preparation to receive new commands to attack a specific target. Meanwhile, the malicious code may also automatically probe the infected PC for personal data, or may log keystrokes, and transmit the information to the botmaster.

The Shadow server Foundation is an organization that monitors the number of command and control servers on the Internet, which indicates the number of bot through May 2007, approximately 1,400 command and control servers were found to be active on the Internet. The number of individual infected drones that are controlled by these 1,400 servers reportedly grew from half a million to more than 3 million from March to May 2007, Symantec, another security organization, reported that it detected 6 million bot-infected computers in the second half of 2006.

4.19 Other Cyber Crime Methods:

Cyber Crime is usually conducted through a connection to the Internet, but can also involve unauthorized removal of data on small, portable flash drive storage devices. Cyber Crime, usually in the form of network hacking, has involved persons with strong technical skills, often motivated by the desire to gain popularity among their technology peers. However, the growing trend is now to profit from these network cyber-attacks by targeting specific systems, often through collaboration among criminals and technical experts. The motives that drive these cybercriminal groups now may differ from those of their paying customers, who may possess little or no technical skills.

New technologies continue to outpace policy for law enforcement. Problems of coordination among agencies of different countries, along with conflicting national policies about crime in cyberspace, work to the advantage of Cyber criminals who can choose to operate from geographic locations where penalties for some forms of Cyber Crime may not yet exist. Sophisticated tools for cyber-attack can now be found for sale or for rent on the internet, where highly organized underground Cyber Crime businesses host websites that advertise a variety of disruptive software products and malicious technical services. High-end Cyber Crime groups use standard software business development techniques to keep their products updated with the latest anti-security features, and seek, to recruit new and talented software engineering students into their organizations.

Where illicit profits are potentially very large, some high-end criminal groups have reportedly adopted standard IT business practices to systematically develop more efficient and effective computer code for Cyber Crime. Studies also show that organized crime groups now actively recruit college engineering graduates and technical expert members of computer societies, and sponsor them to attend more information technology (IT) courses to further their technical expertise. However, in some cases, targeted students may not realize that a criminal organization is behind the recruitment offer.

Cyber attacks are increasingly designed to silently steal information without leaving behind any damage that would be noticed by a user. These types of attacks attempt to escape detection in order to remain on host systems for longer periods of time. It is also expected that as mobile communication devices are incorporated more into everyday life, they will be increasingly targeted in the future for attack by Cyber criminals.

4.19.1 Malicious Code:

Definition:

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

Malicious code, such as viruses or Trojan Horses, are used to infect a computer to make it available for takeover and remote control. Malicious code can infect a computer if the user opens an email attachment, or clicks an innocent looking link on a website. For example, users who visited the popular MySpace and YouTube websites in 2005, and who lacked important software security patches, reportedly may have had their PCs infected if they clicked on a banner advertisement which silently installed malicious code on their computers to log keystrokes or capture sensitive data. During the first half of 2006, the Microsoft Security Team reported that it had removed 10 million pieces of malicious software from nearly 4 million computers and web servers. Recently, analysis at Google tested several million web pages for the presence of malicious software, and determined that 4.5 million of the web pages examined were suspicious in nature. After further testing of the 4.5 million web pages, over 1 million were found to launch downloads of malicious software, and more than two thirds of those program were "bot" software that, among other things, collected data on banking transactions and then emailed the information to a temporary email account.

Researchers at the San Jose, Calif-based security firm, Finjan Inc., after reviewing security data from the first quarter of 2007, found that more malware is hosted on servers in countries such as the US. and UK, than in other countries with less developed e-crime law enforcement policies. Findings from the Finjan 2007 Web Security Trends Report are based on an analysis of more than 10 million unique websites from Internet traffic recorded in the UK, and include the following:

1. Attacks that involve the use of code obfuscation through diverse randomization techniques are growing more numerous and complex, making them virtually invisible to pattern-matching/signature-based methods in use by traditional anti-virus products.
2. Criminals are displaying an increasing level of sophistication when embedding malicious code within legitimate content with less dependence on outlaw servers in unregulated countries.

Finjan found that 90% of the websites examined containing malware resided on servers located in the US or UK "The results of this study shatter the myth that malicious code is primarily being hosted in countries where-e-crime laws are less developed," Finjan CTO Yuval Ben-Itzhak reportedly stated.

4.19.2 Identity Theft:

Botnets and other examples of malicious code can operate to assist cyber criminals with identity theft. Current FBI estimates that identity theft costs American businesses and consumers $50 billion a year. Individual users are often lured into clicking on tempting links that are found in email or when visiting websites. Clicking on titles such as "Buy Rolex watches cheap," or "Check out my new Photos", can take advantage of web browser vulnerabilities to place malicious software onto a users system which allows a cybercriminal to gather personal information from the user's computer.

Malicious code can scan a victim's computer for sensitive information, such as name, address, place and date of birth, social security number, mother's maiden name, and telephone number. Full identities obtained this way are bought and said in online markets. False identity documents can then be created from this information using home equipment such as a digital camera, colour printer, and laminating device, to make official-looking driver's licences, birth certificates, reference letters, and bank statements.

Identity theft involving thousands of victims is also enabled by inadequate computer security practices within organizations. MasterCard International reported that in 2005 more than 40 million credit card numbers belonging to US consumers were accessed by computer hackers. Some of these account numbers were reportedly being said on a Russian website, and some consumers have reported fraudulent charges on their statements. Officials at the UFJ bank in Japan reportedly stated that some of that bank's customers may also have become victims of fraud related to theft of the MasterCard Information. In June 2006, officials from the US Department of Energy acknowledged that names and personal information belonging to more than 1,500 employees of the National Nuclear Security Administration (NNSA) had been stolen in a network intrusion that apparently took place in 2004. The NNSA did not discover the security breach until one year after it had occurred.

Some sources report that stolen credit card numbers and bank account information are traded online in a highly structured arrangement, involving buyers, sellers, intermediaries, and service industries. Services include offering to conveniently change the billing address of a theft victim, through manipulation of stolen PINs or passwords. Observers estimated that in 2005 such services for each stolen MasterCard number cost between $42 and $72. Other news articles report that, in 2007, a stolen credit card number sells online for only $1, and a complete identity, including a US bank account number, credit-card number, date of birth, and a government issued ID number now sells for just $14 to $18.

As of January 2007, 35 states have enacted data security laws requiring businesses that have experienced an intrusion involving possible identity theft to notify persons affected, and to improve security for protection of restricted data. However, existing federal and state laws that impose obligations on information owners, may require harmonization to provide protections that are more uniform.

4.19.3 Cyber Espionage:

Cyber espionage involves the unauthorized probing to test a target computer's configuration or evaluate its system defences, or the unauthorized probing to test a target computer's configuration or evaluate its system defences, or the unauthorized viewing and copying of date files. However, should a terrorist group, nation, or other organization use computer hacking techniques for political or economic motives, their deliberate intrusions may also quality them, additionally, as cyber criminals. If there is disagreement about this, it is likely because technology has outpaced policy for labelling actions in cyberspace. In fact, industrial cyber espionage may now be considered as a necessary part of global economic competition, and secretly monitoring the computerized functions and capabilities of potential adversary countries may also be considered essential for national defence.

4.20 Connection between Terrorism and Cyber Crime:

The proportion of Cyber Crime that can be directly or indirectly attributed to terrorists is difficult to determine. However, linkages do exist between terrorist groups and criminals that allow terror networks to expand internationally through leveraging the computer resources, money laundering activities, or transit routes operated by criminals. For example, the 2005 UK subway and bus bombings, and the attempted car bombings in 2007, also in the UK provide evidence that groups of terrorists are already secretly active within countries with large communication networks and computerized infrastructures, plus a large, highly skilled IT workforce. London police officials reportedly believe that terrorists obtained high-quality explosives used for the 2005 UK bombings through criminal groups based in Eastern Europe.

A recent trial in the UK revealed a significant link between Islamic terrorist groups and Cyber Crime. In June 2007, three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, pleaded guilty, and were sentenced for using the Internet to incite murder. The men had used stolen credit card information at online web stores to purchase items to assist fellow jihadists in the field—items such as night vision goggles, tents, global positioning satellite devices, and hundreds of prepaid cell phones, and more than 250 airline tickets, through using 110 different stolen credit cards. Another 72 stolen credit cards were used to register over 180 Internet web domains at 95 different web hosting companies. The group also laundered money charged to more than 130 stolen credit cards through online gambling websites. In all, the trio made fraudulent charges totalling more than $3.5 million from a database containing 37,000 stolen credit card numbers, including account holders' names and addresses, dates of birth, credit balances, and credit limits.

Cyber criminals have made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where illegal drug funds or other profitable activities such as credit card theft, are used to support terrorist groups. Drug traffickers are reportedly among the most widespread users of encryption for internet, messaging, and are able to hire high level computer specialists to help evade law enforcement, coordinate shipments of drugs, and launder money. Regions with major narcotics markets, such as Western Europe and North America, also possess optimal technology infrastructure and open commercial nodes that increasingly serve the transnational trafficking needs of both criminal and terrorist groups. Officials of the US Drug Enforcement Agency (DEA), reported in 2003 that 14 of the 36 groups found on the US State Department's list of foreign terrorist organizations were also involved in drug trafficking. A 2002 report by the Federal Research Division at the Library of Congress, revealed a "growing involvement, of Islamic terrorist and extremists groups in drug trafficking," and limited evidence of cooperation between different terrorist groups involving both drug trafficking and trafficking in arms. Consequently, DEA officials reportedly argued that the war on drugs and the war against terrorism are and should be linked.

State Department officials, at a Senate hearing in March 2002, also indicated that some terrorist groups may be using drug trafficking as a way to gain financing while simultaneously weakening their enemies in the West through exploiting their desire for addictive drugs. The poppy crop in Afghanistan reportedly supplies resin to produce over 90% of the world's heroin, supporting a drug trade estimated at $3.1 million. Reports indicate that money from drug trafficking in Afghanistan is used to help fund terrorist and insurgent groups that operate in that country. Subsequently, US intelligence reports in 2007 have stated that AL Qaeda in Afghanistan" has been revitalized and restored to its pre-September 11, 2001 operation levels, and may now be in a better position to strike Western countries.

Drug traffickers have the financial clout to hire computer specialists with skills for using technologies which make Internet messages hard or impossible to decipher, and which allow terrorist organizations to transcend borders and operate internationally with less chance of detection. Many highly trained technical specialists that make themselves available for hire originally come from the countries of the former Soviet Union and the Indian subcontinent. Some of these technical specialists reportedly will not work for criminal or terrorist organizations willingly, but may be misled or unaware of their employers' political objectives. Still, others will agree to provide assistance because other well-paid legitimate employment is scarce in their region.

4.20.1 Links between Computer Hackers and Terrorists, or Terrorist Sponsoring Nations may be Difficult to Confirm:

Membership in the most highly-skilled computer hacker groups is sometimes very exclusive and limited to individuals who develop, demonstrate, and share only with each other, their most closely guarded set of sophisticated hacker tools. These exclusive hacker groups do not seek attention because maintaining secrecy allows them to operate more effectively. Some hacker groups may also have political interests that are supra-national, or based on religion, or other socio-political ideologies, while other hacker groups may be motivated by profit, or linked to organized crime, and may be willing to sell their computer services, regardless of the political interests involved. Information about computer vulnerabilities is now for sale online in a hacker's "black market". For example, a list of 5,000 addresses of computers that have already been infected with spyware and which are waiting to be remotely controlled as part of an automated "bot network" reportedly can be obtained for about $150 to $500. Prices for information about computer vulnerabilities for which no software patch yet exists reportedly range from $1,000 to $5,000.

4.20.2 Terrorist Capabilities for Cyber Attack:

Some experts estimate that advanced or structured cyber attacks against multiple systems and networks, including target surveillance and testing of sophisticated new hacker tools, might require from two to four years of preparation, while a complex coordinated cyber attack, causing mass disruption against integrated, heterogeneous systems may require 6 to l0 years of preparation. This characteristic, where hackers devote much time to detailed and extensive planning before launching a cyber attack, has also been described as a "hallmark" of previous physical terrorist attacks and bombings launched by AL Quaeda.

It is difficult to determine the level of interest, or the capabilities of international terrorist groups to launch an effective cyber attack. A 1999 report by the Centre for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School concluded that it is likely that any severe cyber attacks experienced in the near future by industrialized nations will be used by terrorist groups simply to supplement the more traditional physical terrorist attacks.

Some observers have stated that AL Quaeda does not see cyber attack as important for achieving its goals, preferring attacks which inflict human casualties. Other observers believe that the groups most likely to consider and employ cyber attack and cyber terrorism are the terrorist groups operating in post-industrial societies (such as Europe and the United States), rather than international terrorist groups that operate in developing regions where there is limited access to high technology.

4.20.3 Possible Effects of a Coordinated Cyber Attack:

In March 2007, researchers at Idaho National Laboratories (INL) conducted an experiment labelled the "Aurora Generator Test" to demonstrate the results of a simulated cyber attack on a power network. In a video released by the Department of Homeland Security, a power generator turbine, similar to many now in use throughout the United States, is forced to overheat and shut down dramatically, after receiving malicious commands from a hacker. The researchers at INL were investigating results of a possible cyber attack directed against a vulnerability that, reportedly, has since been fixed. The video, vulnerabilities could potentially be disabled the same way.

In July 2002, the US Naval War College hosted a war game called "Digital Pearl Harbor" to develop a scenario for a coordinated cyber terrorism event, where mock attacks by computer security experts against critical infrastructure systems simulated state-sponsored cyber warfare. The simulated cyber attacks determined that the most vulnerable infrastructure computer systems were the internet itself, and the computer systems that are part of the financial infrastructure. It was also determined that attempts to cripple the US telecommunications infrastructure would be unsuccessful because built-in system redundancy would prevent damage from becoming too widespread. The conclusion of the exercise was that a "digital Pearl Harbor" in the United States was only a slight possibility.

However, in 2002, a major vulnerability was discovered in switching equipment software that threatened the infrastructure for major portions of the Internet, a flaw in the Simple Network Management Protocol (SNMP) would have enabled attackers to take over internet routers and cripple network telecommunications equipment globally. Network and equipment vendors worldwide raced quickly to fix their products before the problem could be exploited by hackers, with possible worldwide consequences. US government officials also reportedly made efforts to keep information about this major vulnerability quiet until after the needed repairs were implemented on vulnerable Internet systems. According to an assessment reportedly written by the FBI, the security flaw could have been exploited to cause many serious problems, such as bringing down widespread telephone networks and also halting control information exchanged between ground and aircraft flight control systems.

While describing possible offensive tactics for military cyber operations, DOD officials reportedly stated that the US could confuse enemies by using cyber attack to open floodgates, control traffic lights, or scramble the banking systems in other countries. Likewise, some of China's military journals speculate that cyber attacks could disable American financial markets. China, however, is almost as dependent on these US markets as the United States, and might possibly suffer even more from such a disruption to finances. As to using cyber attack against other US critical infrastructures, the amount of potential damage that could be inflicted might be relatively trivial compared to the costs of discovery, if engaged in by a nation state. However, this constraint does not apply to non-state actors like AL Qaeda, thus making cyber attack a potentially useful tool for those groups who reject the global market economy.

4.20.4 Organized Cyber Crime:

Some large cyber criminal groups are transnational, with names like Shadow-crew, Carderplanet, and Darkprofits, individuals in these groups reportedly operate from locations all over the world, working together to hack into systems, steal credit card information and sell identities, in a very highly structured, organized network. Organized crime is also recruiting teenagers who indicate that they feel safe doing illegal activity online than in the street. A recent report from the McAfee security organization, titled the 'Virtual Criminology Report', draws on input from Europe's leading high-tech crime units and the FBI, and suggests that criminal outfits are targeting top students from leading academic institutions and helping them to acquire more skills that is essential to commit high-tech crime on a massive scale.

In the future, we may see new and different modes of criminal organization evolve in cyberspace. Cyberspace frees individuals from many of the constraints that apply to activities in the physical world, and current forms of criminal organization may not transition well to online crime. Cyber Crime requires less personal contact, less need for formal organization, and no need for control over a geographical territory. Therefore, some researchers argue that ″the classical hierarchical structures of organized crime groups may be unsuitable for organized crime on the internet. Consequently online criminal activity may emphasize lateral relationship and networks instead of hierarchies."

Instead of assuming stable personnel configurations that can persist for years, online criminal organization may incorporate the "swarming" model, in which individuals coalesce for a limited period of time in order to conduct a specific task, or set of tasks, and afterwards go their separate ways. The task of law enforcement could therefore become much more difficult. If Cyber criminals evolve into the "Mafia of the moment" or the "cartel of the day," police will lose the advantage of identifying a permanent group of participants who engage in a set of routine illicit activities, and this will only contribute to the future success of organized Cyber Crime.

Cyber terrorist prefer using the cyber attack methods because of many advantages for it:

- It is Cheaper than traditional methods.
- The action is very difficult to be tracked.
- They can hide their personalities and location.
- There are no physical barriers or check points to cross.
- They can do it remotely from anywhere in the world.
- They can use this method to attack a big number of targets.
- They can affect a large number of people.

अध्याय 5
Chapter 5
Cyber Crime and Punishment

Notes :

5.1 General:

In the era of cyber world, as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term 'Cyber' became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyberspace wherein internet provides equal opportunities to all the people to access any information, data storage, analyze etc with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to Cyber Crimes at the domestic and international level as well.

Cyber Crimes actually means: It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site. Cyber Crimes are not limited to outsiders except in case of viruses and with respect to security related Cyber Crimes that are usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cyber Crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

5.2 Need of Cyber Law:

Information Technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is an expansion in the Cyber Crimes i.e. breach of online contracts, perpetration of online torts and crimes etc Due to these consequences, there is a need to adopt a strict law by the cyberspace authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of Cyber Crime. In the modern cyber technology world, it is essential to regulate Cyber Crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

Since users of computer system and internet are increasing worldwide, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by netizens while using the internet which will assist in challenging this major threat Cyber Crime.

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.

This report analyzes the state of the law in 52 countries. It finds that only ten of these nations have amended their laws to cover more than half of the kinds of crimes that needs to be addressed. While many others have initiatives underway, it is clear, that a great deal of additional work is needed before organizations and individuals can be confident that cyber criminals will think twice before attacking valued systems and information.

5.3 What's different about Cyber Crime?

Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security. Headlines of cyber attacks command our attention with increasing frequency. According to the Computer Emergency Response Team Coordination Centre (CERT/CC), the number of reported incidences of security breaches in the first three quarters of 2000 has risen by 54% over the total number of reported incidences in 1999. Moreover, countless instances of illegal access and damage around the world remain unreported, as victims fear the exposure of vulnerabilities, the potential for copycat crimes, and the loss of public confidence.

Cyber Crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

As this report shows, the laws of most countries do not clearly prohibit Cyber Crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property. New kinds of crimes can fall between the cracks, as the Philippines learned when it attempted to prosecute the perpetrator of the May 2000 Love Bug virus, which caused billions of dollars of damage worldwide.

5.4 Effective Law Enforcement:

Effective law enforcement is necessary to enact and implement alcohol control policies which affect underage access to alcohol so as to reduce underage access, overall. Without such enforcement, communities may begin to view alcohol control policies as meaningless and violations of such policies as acceptable.

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting Cyber Crimes.

Six weeks after the Love Bug attack, the Philippines outlawed most computer crimes as part of a comprehensive e-commerce statute. In order to prevent a repeat of the catastrophe that prompted this action, however, the future of the networked world demands a more proactive approach, whereby governments, industry, and the public work together to devise enforceable laws that will effectively deter all but the most determined cyber criminals.

5.5 Poor Information Security Reduces the Competitiveness of Nations:

Security is a concept everyone is familiar with. We prevent unwanted people from entering our houses and cars using locks and alarm systems. Computer security is no different.

To illustrate computer security, look at most modern office buildings. There are two basic ways a company can enforce security, and a third hybridized method. The first way is accomplished by placing security guards at the front door and at every door within the building that access needs to be restricted. Employees are assigned an identification card. When the employee wishes to enter the building or a door, the guard examines the ID. First, the guard verifies that the employee is who the person on the ID card is. This is authentication — verification of a person's identity. Next, the guard checks a list of "allowed people". If the employee is on the list, he is permitted access. Changes in employee access is achieved by the addition or removal of his name from a particular guard's list.

In August 2000 report, Risk E-Business: Seizing the Opportunity of Global E-Readiness, McConnell International rated mid-level economies’ capacity to participate in the digital economy. In considering nations’ information security, the report evaluated public trust in the security of information processed and stored on networks in each country. In this context, information security included; an assessment of the strength of legal protections and progress in protecting intellectual property rights, especially for software; the extent of efforts to protect electronic privacy; and the strength and effectiveness of the legal framework to authorize digital signature. The E-Readiness report also examined the existence of legal frameworks to prosecute cyber criminals, for a predictable environment of strong deterrence for computer crime is critical to the effective protection of valuable information and networks.

Although several countries, particularly in Europe and Asia, were found to have addressed a number of these broader information security factors, few countries were able to demonstrate that adequate legal measures had been taken to ensure that perpetrators of Cyber Crime would be held accountable for their actions. Overall, nearly half of the countries included in the E-Readiness study were rated as needing substantial improvement in information security. In addition, only a small fraction of countries needing substantial improvement indicated that progress was currently underway.

Outdated laws and regulations, and weak enforcement mechanisms for protecting networked information, create an inhospitable environment in which to conduct e-business within a country and across national boundaries is difficult. Inadequate legal protection of digital information can create barriers to its exchange and stunt the growth of e-Commerce. As e-Business expands globally, the need for strong and consistent means to protect networked information will grow.

5.6 Law is Only Part of the Answer:

Extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and businesses. Because that extension remains a work in progress, organizations today must first and foremost defend their own systems and information from attack, be it from outsiders or from within. They may rely only secondarily on the deterrence that effective law enforcement can provide.

To provide this self-protection, organizations should focus on implementing cyber security plans addressing people, process, and technology issues. Organizations need to commit the resources to educate employees on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology—such as firewalls, anti-virus software, intrusion detection tools, and authentication services —throughout the organizations' computer systems.

These system protection tools — the software and hardware for defending information systems — are complex and expensive to operate. To avoid hassles and expense, system manufacturers and system operators routinely leave security features "turned off", needlessly increasing the vulnerability of the information on the systems. Bugs and security holes with known fixes are routinely left uncorrected. Further, no agreed — upon standards exist to bench mark the quality of the tools, and no accepted methodology exists for organizations to determine how much investment in security is enough. The inability to quantify the costs and benefits of information security investments leave security managers at a disadvantage when competing for organizational resources. Much work remains to improve management and technical solutions for information protection.

Industry-wide efforts are underway to address prevention, response, and cooperation. Around the world, various industries have been establishing information sharing and analysis centres (ISACs) to share real-time information related to threats, vulnerabilities, attacks, and countermeasures. A recent Global Information Security Summit sponsored by the World Information Technology and services Alliance (www.witsa.org) brought together industry, governments, and multilateral organizations across economic sectors to share information and build partnerships. Post-summit working groups are now developing cooperative approaches to addressing the most critical information security problems. The results of that work will be taken up at a second summit in Belfast in May 2001. That summit will also provide an opportunity to resist the progress of nations in updating their laws to cover Cyber Crimes.

5.7 Miscellaneous:

The word miscellaneous comes from the Latin word *miscere*, meaning "to mix." You might have heard the expression "a mixed bag," which applies when you don't quite know what you're going to get. That's true of a bag of miscellaneous objects, too. You might pull out socks and a stick of butter — two things that don't seem to go together. Similarly, miscellaneous can describe something with many variations, like a person who expresses herself in many different ways.

5.7.1 Reliance on Terrestrial Laws is an Untested Approach:

Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute Cyber Crimes. The majority of countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in Court.

5.7.2 Weak Penalties Limit Deterrence:

The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects.

5.7.3 Self-Protection Remains the First Line of Defence:

The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.

5.7.4 A Global Patchwork of Laws Creates Little Certainty:

Little consensus exist among countries regarding exactly which crimes need to be legislated against. In the networked world, no island is an island. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat Cyber Crime will be complicated.

5.7.5 A Model Approach is Needed:

Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for e-commerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public — private partnership to produce a model approach can help in eliminating the potential danger from the inadvertent creation of Cyber Crime havens.

5.8 Recommendations:

The weak state of global legal protections against Cyber Crime suggests three kinds of action.

5.8.1 Firms Should Secure their Networked Information:

Laws to enforce property rights work only when property owners take reasonable steps to protect their property in the first place. As one observer has noted, if home owners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police? Even where laws are adequate, firms dependent on the network must make their own information and systems secure. And where enforceable laws are months or years away, as in most countries, this responsibility is even more significant.

5.8.2 Governments Should Assure that their Laws Apply to Cyber Crimes:

National governments remain the dominant authority for regulating criminal behaviour in most places in the world. One nation already has struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by Cyber Crime.

It is crucial that other nations profit from this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals. In many cases, nations will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat.

5.8.3 Firms, Governments and Civil Society Should Work Cooperatively to Strengthen Legal Frameworks for Cyber Security:

To be prosecuted across a border, an act must be a crime in each jurisdiction. Thus, while local legal traditions must be respected, nations must define Cyber Crimes in a similar manner. An important effort to craft a model approach is underway in the Council of Europe (see www.coe.int), comprising 41 countries. The Council is crafting an international Convention on Cyber Crime. The Convention addresses illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes. It also addresses investigational matters related to jurisdiction, extradition, the interception of communications, and the production and preservation of data. Finally, it promotes cooperation among law enforcement officials across national borders.

Later in its process, the Council began to consider the views of affected industry and civil society. This process is making the Council's product more realistic, practical, efficient, balanced, and respectful of due process that protects individual rights. At this point, most observers support provisions to improve law enforcement cooperation across borders. However, industry, through the World Information Technology and Services Alliance (see www. witsa.org/press/), argues that the requirements on service providers to monitor communications and to provide assistance to investigators, as outlined in the Draft Convention, would be unduly burdensome and expensive. Another provision considered objectionable could criminalize the creation and use of intrusive software, or hacking programs, which are designed for legitimate security testing purposes. This action could stifle the advances in technology vital to keep up with evolving cyber threats. Privacy and human rights advocates (see www.gilc.org) object to the Draft Convention's lack of procedural safeguards and due process to protect the rights of individuals, and to the possibility that the ensuing national laws would effectively place restrictions on privacy, anonymity, and encryption.

The Council plans to release a final draft of the Convention in December 2000. In 2001, a political process involving national governments will determine the scope and coverage of the final Convention. Because of Cyber Crime's international potential, all countries, and all companies, are affected. Interested parties, including national governments from outside Europe, and businesses and non-governmental organizations from around the world, should participate vigorously in a consensus process to develop measures that support effective international law enforcement and foster continued growth and innovation.

अध्याय 6
Chapter 6
Investigation of Computer Crime

Notes :

6.1 General:

Anyone who has an Internet account knows that the ISP is a subscription service that grants the user access to the Internet. What most people, including many crooks and cops, don't know is that ISPs have records of everything; a subscriber does on the Internet. That's the good news for investigators. The bad news is that the records are digital information with a very finite existence. In other words, if you're investigating a Cyber Crime involving the Internet, you better move fast. How fast depends on the policy of the ISP in question. Large ISPs often keep their data as much as 30 days, but that's not true in all cases. Data storage is a major cost centre for ISPs, and some save money by dumping the data very quickly. Once we sent a subpoena to an ISP, requesting their records, and their answer was, "Sorry. We only keep our records for 30 minutes."

Because ISPs would rather dump data than store it, one of the most important weapons in a Cyber Crime investigator's arsenal is a letter requesting that the ISP preserve the data until the investigator can secure a subpoena, warrant, or court order requiring the ISP to turn over its records. The preservation letter does not legally require the ISP to turn over its records. But many ISPs will cooperate with a request to preserve data. Once you get the records from the ISP, you're probably in business. In order to subscribe to the service, the auction thief had to give personal information like his or her physical address. Yes, they can use false information and fake credit cards, but even that information can be valuable. When you have an address and a name for the suspect, your investigation is likely to involve another agency. Cyber Crimes are not like in-person physical crimes. The victim is often in another state from the suspect. And that means you may work for the Chennai Police Department and suddenly need to serve a warrant in Bangalore. Experienced cyber police say that jurisdictional disputes are rare occurrences during Cyber Crime cases and that other agencies are likely to cooperate with your investigation.

The investigation of these computer crimes and the gathering of appropriate evidence for a criminal prosecution can be extremely difficult and complex issue, due to intangible, often transient nature of the data, especially in a networked environment. Criminals often leave no trace. Sometimes evidence is removed by introduction of viruses, computer investigation requires a considerable amount of time also because of the large volume of data to be scanned for detecting the crime and for evidential purposes. The investigations also involve interactions with victims. Victims could be experts and sometimes the perpetrators of the crime themselves.

6.2 Administrative Mechanism:

As said earlier that the problem in investigation of computer crime is more technological, economical and infrastructural than legal. In order to deal with Cyber Crimes the first Cyber Crime police station was opened in Bangalore. After Bangalore even Mumbai, Delhi and Hyderabad also have established Cyber police stations to handle Cyber Crime. The Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI) is also one of the specialized investigation bodies. The jurisdiction of this cell is throughout India, besides the offences punishable under Chapter XI of the IT Act 2000. It also has the power to look into other high tech crimes. The CCIC functions under the overall guidance of Special Director, Joint Director, Economic offences Wing II and the immediate supervision of the Deputy Inspector General of Special Investigation Cell-III. The Cell is headed by a Superintendent of Police, three Inspectors and one Sub-Inspector at present, besides other supporting staff.

6.3 Anonymity of Cyberspace:

Anonymity in cyberspace is a major concern for the global community. The introduction, growth and utilization of information and communications technologies (ICTs) have been accompanied by an increase in criminal activities. With respect to cyberspace, identities are easily cloaked in anonymity. Once a message sender's identity is anonymous, cyberspace provides the means to perpetrate wide spread criminal activity to the masses, with little chance of apprehension. On the other hand, anonymity in cyberspace allows whistle-blowers and political activists to express opinions critical of employers and the government enables entrepreneurs to acquire and share technical information without alerting their competitors, and permits individuals to express their views online without fear of reprisals and public hostility.

Anonymity is one of the celebrated gifts of cyberspace; it helps in greater flow of information. But however this freedom is misused and is encouraging criminal activities in the Cyber world. After long process of investigation, the criminal is traced with its identity on the internet which proves to be unauthentic and leaves the authorities clueless. The time has now come to regulate this freedom in the interest of society.

6.4 Cognizable & Non-Cognizable Case:

A cognizable offence is a case where the Police can arrest without a warrant. All cognizable cases involve criminal offences. Murder, Robbery, Theft, Rioting, Counterfeiting etc are some examples of cognizable offences. Non-cognizable offences are those criminal infractions, which are relatively less serious. Examples of non-cognizable offences include Public Nuisance, Causing Simple Hurt, Assault, Mischief etc

A constant and assertive distinction is made between a cognizable and a non-cognizable case, this will apply *mutatis mutandis* to an investigation of computer crime. The punishment prescribed under the IT Act will ascertain the same. This decision will also have a bearing on the investigation of a Cyber Crime and the powers of the investigating officer concerned. The police can arrest a person accused of offences under the IT Act, which are punishable with imprisonment for three years or more without a warrant. However Section 80 of the IT Act is an exception to it. Under Section 80(1) the Dy IT SP can arrest any person irrespective of the above distinction if offence is committed in public place.

6.5 Development of Technology:

In the not-too-distant past, a developing nation tended to be seen as a country that lacked access to modern technology.

Today, increasing globalization means that rapid communication; market forces and lower import restrictions can help in making a new technology available anywhere that might be useful.

The biggest impact has come from ICTs — the computers, mobile telephones and satellite communications at the core of the modern information society.

Wide disparities in access still exist, due to both economic reasons and deficiencies in physical infrastructure. One of the main reasons for the slow penetration of the Internet in Africa, for example, is the reliance on slow, expensive and often unreliable copper wire connections instead of high-speed fibre optic cabling.

In UK, a Foresight Project on Cyber Trust and Crime Prevention in 2004 was accomplished. The project explored the application and implications of the new generation of ICT's across a variety of areas and the possibility and challenges they bring for crime prevention in the future. These areas included identity and authenticity system robustness and depend-ability security and information assurance and privacy and surveillance.

6.6 Duties of Active Co-operation:

In the traditional systems of evidence collection, there are two instruments that are being relied upon by investigating agencies to effectuate investigation and evidence collection, i.e. duty to surrender seizable objects and the duty to testify. Duty to surrender is covered under Section 91 of Cr PC which obligates a person having the document or any such matter to surrender it, when the Court issues summons or when an investigating officer directs by a written order. Also Section 100(1) confers a duty upon persons in charge of a place where the investigation is carried out to provide access to such place and to help officers in all possible manners. Duty to Testify is the second important instrument of active co-operation. The Cr PC contains provisions as to the power of investigating officer to require attendance of witness and their examination. In United Kingdom also under the Police and Criminal Evidence Act, 1984 of the United Kingdom confers a duty on the person that the constable may require any information which is contained in the computer.

6.7 Duty of Intermediaries:

Intermediaries operating in real world who facilitate use of virtual world have a duty of active co-operation under the Cr PC but it's not sufficient. Contemplate a situation if a telecommunication company or an intermediary does not keep records of the type for which a search warrant is issued and a warrant allowing a very wide retrieval would be excessively intrusive into privacy of third party. As a matter of practice most of the cyber cafe owners do not keep a proper record of its customers, during investigation this creates a problem. Further they cannot be even asked to generate records. Hence law should impose some duty on these intermediaries to keep record of their customers.

6.8 Investigation of Cyber Crimes:

This five-day, hands-on course is designed to prepare investigators for investigating Cyber Crime. This course is designed to serve as an introductory course, providing exposure to the various types of Cyber Crime, how to plan and prepare for Cyber Crime activity, the methodologies and tools used to investigate Cyber Crime, as well as how to manage the computer crime scene. The course utilizes instructor-led discussion and instruction, and is reinforced with a number of exercises and hands-on practical exams. The course concludes with a practical exam scenario, which will require the students to apply the skills they have learned throughout the week.

The investigation of Cyber Crimes is complex. The evidence is often in an intangible form. Its collection, appreciation, analysis arid preservation present , unique challenges to the Investigator. The increased use of networks and the growth of the Internet have added to this complexity. Using the Internet, it is possible for a person sitting in India to steal a computer resource in Brazil using a computer situated in USA as a launch pad for his attack. Distributed attacks are also not unheard of. The challenges in such cases are not only technological, but also jurisdictional.

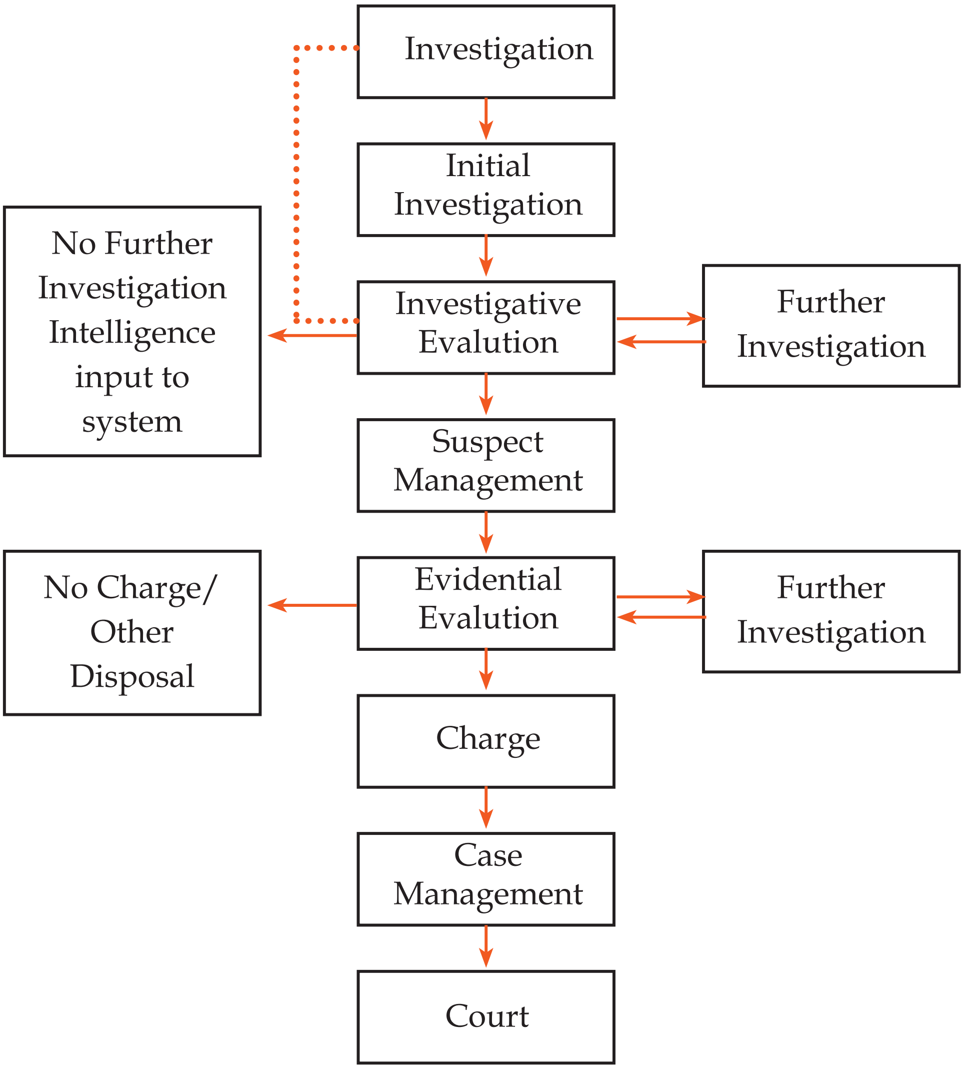


Fig. 6.1. Investigation Process — Computer Crime

Whatever we treasure for ourselves separates us from others; our possessions are our limitations.
- Swami Vivekananda

Of late, we are experiencing more and more of Cyber Crimes, since many of us have switched over to the fourth mode of communication i.e. Internet from the previous modes viz. gestures, speech and writing. The internet has opened up avenues of commerce, trade and communication like never before. It is the network that deals in billions of transactions each day. These transactions are usually transactions of money, pictures, information and videos. The magnitude of transactions—the sheer volume makes internet not just an easy tool for information exchange, but also an ideal hotbed of crimes.

Cyber Crime being technology driven evolves continuously and ingeniously making it difficult for investigators to cope up with changes. Criminals are always one step ahead in the sense that they create technology or come up with technique to perpetrate a particular crime and the law enforcers then counter such techniques or technologies.

6.9 Lack of Expertise:

Basis of credibility of a person who is perceived to be knowledgeable in an area or topic due to his or her study, training, or experience in the subject matter. The police substantially lack in basic skills required for investigating computer crimes, unless training is imported or experts are appointed for investigation, investigation is a hard nut to crack. This problem was highlighted by the Malimath Committee also, and it recommended that proper training of police officials is necessary. It even recommended that in order to investigate high tech offences like Cyber Crime special cells must be established. Even a separate intelligence network should be established. We don't have experts in our investigation process, so we must recruit - cyber forensic experts now. In US in the State and local level, law enforcement departments are hiring computer forensics specialists. In connection to experts author John R. Vacca mentions certain requirements which he must be able to perform: (1) Data seizure; (2) data duplication and preservation; (3) data recovery; (4) document searches; (5) media conversion; (6) expert witness services; (7) computer evidence service options and (8) other miscellaneous services.

6.10 Lack of Funds and Resources:

This is a genuine problem which is witnessed in every other jurisdiction, even in developed countries. This is also a major problem in India, where the policemen are not equipped with proper gadgets and weapons even to combat with regular crimes and criminals, to expect in the field of computer crimes seems to be a utopia. Unless adequate funds are available, we cannot have developed technologies, advanced laboratories, proper gadgets and even training of officials.

6.11 Lack of Sensitivity:

The magnitude of a financial instrument's reaction to changes in underlying factors. Financial instruments, such as stocks and bonds, are constantly impacted by many factors. Sensitivity accounts for all factors that impact a given instrument in a negative or positive way in an attempt to learn how much a certain factor will impact the value of a particular instrument.

Lack of sensitivity by the investigating authorities is also resulting in encouragement of these activities. Police often say, "we have far more important cases of murder, rape, dacoity to deal with". Practically police don't take cases of computer crimes on priority. They either go unattended or are delayed which gives the criminals enough time to delete traces of their crime.

6.12 Legal Framework:

The General Assembly of the United Nations by resolution A/RES/S1/162, dated 30-1-1997 has adopted the Model Law on Electronic Commerce of UNCITRAL. To effectuate this, Indian Parliament enacted the Information Technology Act 2000 (hereinafter sometimes abbreviated as IT Act). According to McConnell International Survey out of 52 countries surveyed India is one of those 10 countries which had substantially updated its Cyber Crime laws. The legal framework in India for investigating computer crime is scattered in the IT Act 2000 read along with The Criminal Procedure Code, 1973. All the basic principles of our Criminal Procedural Law are applicable *mutatis mutandis* to computer crimes.

6.13 Local Jurisdiction:

Jurisdiction is the right of the court to hear a specific case. For a criminal case, the court where the trial takes place must be correct for the trial to be valid. Criminal jurisdiction is based on certain factors: the place where the crime took place, the type of case and the subject matter.

The rule of local jurisdiction will also apply in case of investigation of an offence under the IT Act. Chapter XII of Cr PC provides that a case is to be investigated by the police officer in charge of the police station. In cases of offences under the IT Act the Dy SP having jurisdiction over the police station within the local limits of which the offence or part thereof has been committed will investigate the matter.

6.14 Mechanism for Online Surveillance:

Information technologies, and in particular the internet, have brought about fundamental changes in how our society functions. Perhaps the most fundamental of these changes is in the ways in which we communicate; whilst the ability of computers to store and process data has expanded rapidly it is, arguably, the rise of instant, global data transfer that has had the most far-reaching effects.

E-mail, instant messaging, and peer-to-peer file transfers, combined with the digitisation of content, have changed how we experience the world, the means by which we access information, and the shape of our social networks.

The general - purpose nature of computing and telecommunications has, necessarily, resulted in applications of these technologies that are undesirable, illegal and socially unacceptable. There are crimes that are unique to the Internet, such as hacking or distributed denial of service attacks against websites, but in many cases the internet simply provides a new medium for more traditional crimes: blackmail, fraud, or dealing in stolen property such as credit cards.

Surveillance will involve a conflict between privacy and Government interest. Surveillance is often considered to be an infringement of cyber privacy, but the recent past reflects how cyberspace has failed to regulate itself which in turn invites some control and regulation by the Government to monitor criminal activities in cyberspace. Surveillance is a preventive step as it

"Dare to be free, dare to go as far as you're thought leads, and dare to carry that out in your life."

will reduce the chances of Cyber Crime and will also help in detection of crimes at the earliest. Surveillance can reduce the low-level organized crime or opportunistic crimes, in cyberspace which covers actually major chunk of the Cyber Crimes. But organized Cyber Crime of high level, cannot be prevented through Surveillance so it has its own limitations.

6.15 Online First Information Report:

Recently in India the system of filing online FIR was launched. This system may prove to be beneficial to expeditiously deal with computer crimes. Online FIR will bring the matter immediately into the notice of law enforcement agencies and hence will help greatly if spontaneous steps are taken in detection of the crime.

6.16 Power of Interception:

In case of Cyber Crimes power of interception is one of the fundamental powers which the investigating authority must possess. The IT Act conferrers this powers, but not to the investigating authority. In case of interception, the general requirement of physical presence of investigator in case of search is infeasible. For static information search is to be deployed and for moving data interception is intelligible. However, to avoid confusion demarcation between search and interception should be clearly made.

6.17 Power to Investigate Extra-Territorial Offences:

The IT Act has been given extra-territorial effect, and if any offence is committed under the Act the person will be liable irrespective of nationality or irrespective of territorial limits of India, if the offence involves computer or computer system or computer network located in India. So the police have now got the power to also investigate an offence if committed outside without on operation of the other country where the investigation is to be effectuated.

6.18 Premature Action:

Chapter XI of the Cr PC confers powers for preventive action. It is broadly applicable to cognizable offence. A person could be arrested and prevented from committing a cognizable offence at a private or public place. These provisions are applicable to the offences under the I.T Act also and a similar action, subject to Section 78 may be taken under the IT Act (i.e. only by Dy SP) Section 80 of the IT Act provides for preventive actions and confers special powers and any person can be arrested on reasonable suspicion. However it is applicable to the public places only and would apply irrespective of the facts whether the offence about to be committed at the public place is cognizable or non-cognizable.

6.19 Problem of Jurisdiction and Lack of International Co - Operation:

The internet has provided computer crimes an international colour and hence the central issue in all Cyber Crimes is jurisdiction. The offenders often knowingly take benefit of this lacuna. For an effective investigation, the first step is to check whether, there exists a bilateral or multilateral legal instrument often called as Mutual Legal Assistance Treaty (MLTA) between the countries to facilitate evidence gathering. In case of MLTA's (one good example is European Convention on Cyber Crime) time is saved and in absence of such arrangement, delay is caused which in turn may be fatal to the investigation process. Peculiarities of legal systems further complicate the problem of investigation, an action which may be crime in one jurisdiction may not be a crime in other legal system, or may invite a lesser punishment or vice-versa. There are administrative problems also, to effectuate investigation on foreign land, seize materials and collect evidence. During Investigations, remote cross border searches/investigations are also possible, but that may infringe sovereignty, property or privacy protection, even without physically crossing the borders, hence it requires caution. In this regard the European Convention on Cyber Crime provides that if a system is open to public access then there is no infringement, or otherwise to obtain consent of the person who is having lawful authority to disclose the data. In absence of any treaty extradition is a problem, which can hinder the investigation process since at times the accused can provide important clues or factual inputs to the case. In Indian scenario we don't have such bilateral or multilateral treaties. Till now we haven't felt the need, but the future ahead demands to have such arrangements.

6.20 Recommendations of Expert Committee:

An expert committee was constituted by the Central Government. The committee has recommended that Section 80 of the Information Technology Act 2000 which provides wide power to investigating authorities to enter search and even seize the desired material in public places, to be deleted which provided wide powers susceptible to abuse and in order to secure privacy of individuals.

However, the author is of the opinion that such power is necessary in order to search and investigate regarding every offence, since in cases of computer crime speed is the key, if such preventive power is not given keeping in mind the nature of computer crime it will be fatal for investigatory process and for prosecution. Without this power an investigating officer in order to do search, will have to obtain a search warranted if it is a non-cognizable offence since some of the offences under the IT Act are non-cognizable in nature, though they demand quick action. Denial of such power is no solution, but, power properly channelized and safeguarded is the need of the hour. In UK the Regulation of Investigatory Powers Act (RIPA) was passed in the year 2000, clues can be taken from that to channelize the investigation process in cases of computer crimes.

6.21 Recommendations of Malimath Committee:

The Malimath Committee on reforms in criminal justice system gave certain recommendations which are very relevant in the context of investigation of computer crimes they are—

1. Investigation: The Committee recommended that there should be specialized Cyber Crime squad in every State crime branch.
2. Intelligence Network: It further recommended that concrete steps ought to be taken to institutionalize criminal intelligence system and the main task of such body would be to collect, collate and disseminate information about major criminal gangs operating in the country involved in Cyber Crimes, and other organized crime. It would have a computerized data base, accessible to all State Police forces/central agencies.

3. Training of officials: The committee heavily recommended that facilities should be developed for imparting training in modern disciplines such as Forensic Accounting and Information Technology for Cyber Crime.

6.22 Search and Seizure:

In the last decade, personal computers have become an increasingly important source of evidence in criminal cases. Computers record and store a remarkable amount of information about what users write, see, hear, and do. In a growing number of cases, searching the suspect's personal computer is an essential step in the investigation. The thorny issue for the courts — and the fascinating issue for scholars — is how the Fourth Amendment should regulate the process. How does the Fourth Amendment govern the steps that an investigator takes when retrieving evidence from a personal computer? At present, the answer is surprisingly unclear. Lower courts have just begun to grapple with the question, resulting in a series of tentative and often contradictory opinions that leaves many answers unresolved.

The Cr PC lays down the procedure for Search and Seizure under Section 91 to 103. Under the IT act Section 80 empowers the Dy. SP to enter any public place search and arrest any person on reasonable suspicion without a warrant. The provision further provides that the Cr PC shall apply in relation to the entry search or arrest made under the Act. It was this provision, for search without warrant in public places, which caused a stir during the discussions on the Bill just prior to passing it into law. However, the provision was passed untouched. The purpose of a clause of such nature is clearly to undertake quick preventive action, to control the misuse of public Internet access systems such as those found at cyber cafes. This provision is inapplicable for search and seizure at private places. It must be noted that both the powers of investigation and this special power of search is relatively given to a high placed police official i.e. Dy. SP or above, and this is done with the acknowledgement that these wide ranging powers should be exercised responsibility.

The procedure under Cr PC is inadequate in respect to computer crimes as it should provide the procedure to be followed for search and seizure, such as for seizing the system, making copies of files etc it should be laid down specifically because of the ambiguity surrounding computer related evidence and the volatility of computer files.

6.23 Search Warrant:

A search warrant can be issued under Section 93 of Cr PC the Warrant can be specific or general as the case may be. The warrants issued in cases of computer crime investigation can also be resisted on technical ground. The warrants issued may call for a specific information related with a particular computer crime however in order to gather that information from computer devices, may require seizure of that device or even a part of it and then a detailed expert examination of whole records and material stored in the storage device, which will include even the information that is irrelevant but may be sensitive in nature example personal in nature related to reputation, or trade secrets, or records of other economic activities. The seizure of the same may lead to infringement of right to privacy. So the question arises as how to issue matter specific warrants, or how to counter privacy infringement objections.

Yet another problem may arise in case of search without warrant under Section 80 of the IT Act of any public place, as per the principles of our procedural criminal law when a search without warrant is conducted, suit has to be specific search only and there must be reasonable grounds for belief which should be reduced in writing. In Germany, the German provisions related to surveillance provide that all materials obtained are kept under judicial control and police is allowed access to that material which is relevant for them. In UK, to remedy this, Government made changes in the Criminal Justice Police Act, 2001. The Act grants law enforcement agencies the right to remove material, including material potentially outside the scope of the warrant, where it is not reasonably practicable.

6.24 Some Common Mistakes which are Fatal in Investigation:

The lack of technical knowledge and special forensic skills in the investigating officers causes many mistakes during these investigations. Some of the common mistakes are narrated below.

1. Investigators often commit the mistake of working with the same computer which is the object of investigation. Even turning on this computer should be avoided as far as possible since it may contain traps for destroying the information on attempted logins with incorrect password.

2. Investigators usually allow the user or owner to access the compute for his help, which may allow them to destroy the possible proof under the very nose of investigators. To avoid such possibilities, it is necessary to make reserved copies before any one is given access to the computer under investigation.

3. With the purpose of checking viruses and program marks presence in the computer, it is necessary to load the computer from previously prepared diskette, or from stand hard disk and not from its operative system, but all the information transmitters, i.e. CD, DVD, hard disk, diskettes must be checked. A specialist, with the help of special software, should do this kind of work.

4. Extracted matter is properly handled and protected from later mechanical or electromagnetic damage.

5. A record of all processes applied to the computer-based evidence should be created and preserved, so as to allow an independent third party to examine those processes and achieve the same result.

6.25 Special Investigation:

Consequent to the recommendations of the Police Commission 1902, Criminal Investigation Department (CID) was created in Madras Presidency on 18th August 1906 with a sanctioned strength of 1 Deputy Inspector General of Police (DIG), 6 Inspectors, 6 Sub-Inspectors, 12 Head Constables and 12 Constables. The objective of the CID was to tackle inter-district criminals, professional offenders and tribes who were addicted to crime. The CID was bifurcated into

"In a day, when you don't come across any problems - you can be sure that you are travelling in a wrong path"

Special Branch CID and Crime Branch CID in the year 1929. The CB CID was placed under the overall charge of the Inspector General of Police and under direct supervision of DIG Railways, CID and Eastern Range. One Assistant Inspector General of Police Crime Branch was posted to assist the DIG. The executive strength of the CB CID consisted of 1 Superintendent of Police, 4 Inspectors, 4 Sub Inspectors, 6 Head Constables and 19 Constables.

The exception provided in Section 78 of IT Act is that the offences under the IT Act can be investigated only by a police officer not below the rank of Dr SP. However, this exception is only restricted to investigation but so far as other aspects are concerned, the authority mentioned under Cr PC will have the power, ex. to arrest a constable or any police officer in charge will have the power to arrest. The Act has removed the difficulty of fixing criminal liability on Companies in respect of offences committed under the Act as faced under IPC consequently applicability of Cr PC has been extended to such offences. However, it is pertinent to note that special investigation is sought only in cases of crimes committed under the IT Act whereas all other computer crimes will invite normal orthodox investigation procedure if covered under IPC.

Notes :

अध्याय 7

Chapter 7

Cyber Terrorism and Cyber Attack

Notes :

7.1 What is Cyber Terrorism?

In the wake of the recent computer attacks, many have been quick to jump to conclusions that a new breed of terrorism is on the rise and our country must defend itself with all possible means. As a society, we have a vast operational and legal experience and proved techniques to combat terrorism, but are we ready to fight terrorism in the new arena — cyberspace?. A strategic plan of a combat operation includes characterization of the enemy's goals, operational techniques, resources, and agents. Prior to taking combative actions on the legislative and operational front, one has to precisely define the enemy. That is, it is imperative to expand the definition of terrorism to include cyber-terrorism.

Cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Even though the issue of cyber terrorism has attracted huge attention from cyber criminologists, cyber law specialists and social science researchers, very few researches have been done for analyzing the legal issues involved in cyber terrorism in India. Globally, the issue of cyber terrorism has been analyzed from four main angles, namely the missions that are involved in cyber terrorism, the methods that are followed for achieving the ultimate purpose of cyber terrorism, the results of cyber terrorism and the role of laws in combating cyber terrorism.

Most of the researches have shown that usage of cyberspace by terrorist organizations has a three folded purpose, to spread the threat, to gain maximum information about the target government and the governmental property in case damage to property and civil society is also aimed for and to 'recruit' new forces. Some researchers have established that cyber terrorism includes two main types of activities, viz., Cyber Crime and misuse of information technology, and therefore it would be wrong to assume that cyber terrorism is a new kind of Cyber Crime. It may be worthy to note that the types of Cyber Crimes that are involved in cyber terrorism may vary from identity theft, to denial of service attack.

Cyber Crime is a crime that is enabled by, or that targets computers. Some argue there is no agreed-upon definition for "Cyber Crime" because "cyberspace" is just a new specific instrument used to help in commiting crimes that are not new at all. Cyber Crime can involve theft of intellectual property, violation of patent, trade secret, or copyright laws. However, Cyber Crime also includes attacks against computers to deliberately disrupt processing, or may include espionage to make unauthorized copies of classified data. If a terrorist group were to launch a cyber attack to cause harm, such an act also fits within the definition of a Cyber Crime. The primary difference between a cyber attack to commit a crime or to commit terror is found in the intent of the attacker, and it is possible for actions under both labels to overlap.

Cyber terrorism can be defined in different ways viz. it can be politically motivated by hacking operations intended to cause grave harm such as loss of life or severe economic damage or it can be unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

It can be a physical attack that destroys computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard.

Some experts believe that there has been no evidence of a true cyber terrorist attack as defined above. Despite the horrific acts of terrorism that have occurred over the last couple of decades, it appears that none of them fits the prevailing definition of a politically motivated computer intrusion causing loss of life or serious economic damage.

Computers have become an enabling tool, another type of weaponry if you will, for what we might call information warfare or Cyber Crime. Regardless of our working definition—cyber terrorism or Cyber Crime — the potential for creating economic damage is great.

7.2 Evolution of Cyber Terrorism:

Terrorism is continually changing. While at the surface it remains "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear…" it is rapidly becoming the predominant strategic tool of our adversaries. As terrorism evolves into the principal irregular warfare strategy of the 21st century, it is adapting the changes in the world socio-political environment. Some of these changes facilitate the abilities of terrorists to operate, procure funding, and develop new capabilities. Other changes are gradually moving terrorism into a different relationship with the world at large.

Cyber terrorism can be traced since 1944 June attack on the communication system and logistic support of Germany. Thereafter in the era of Second World War, 1945 to 1991 fall of Soviet Union and "Cold War" in 1960s the USA Defence Department started Internet and computer network and thereafter evolved Protocol and ICANN system to regulate cyberspace. By that time in 1960-s to 1980-s hackers took their own shape in Information Super highway. In 1988, Osama Bin Laden established "Al-Qaeda" based on "Jihad". In 1988, West German hackers accessed Department of Defence systems of the USA. Thereafter, "Gulf War" was the first information war or I-war through Information Way or I-way. The USA passed the Nation Infrastructure Protection Act, 1990 to control cyber terrorism. In Europe, the I-way became popular in the year 1998. The United Kingdom (UK) established the Defence Evaluation and Research Agency in the year 1998. Then, Sweden, Norway Finland, Switzerland, Germany, France came forward to combat cyber war. By 1990, Internet became popular through World Wide Web (www) .www became very popular in India in 1995, before that the LTTE groups work was dependent on websites and internet.

7.3 Modes of Cyber Terrorism:

7.3.1 Attack on National Security:

The clear and present danger of cyber threats to our critical infrastructure, such as the national power grid, can no longer be ignored. Fortunately, the government began calling attention to cyber risks in the form of a recent presidential Executive Order, the reintroduction of cyber security legislation, and some long-delayed but honest pronouncements about ongoing attacks from China and other nation-states. Now it is time to move from rhetoric to action.

National security depends on confidentiality, secret information, etc and when terrorists attack them, they destroy, delete or modify those information or purport to do the same and all these are treated as terrorist attack or cyber terrorism.

7.3.2 Cyber Terrorism is the Forerunner of Warfare:

In contemporary era of communication, convergence and new technology, one nation causes terrorist violence against other nation or nations by using or making the target of new technology. This is called net war or warfare. For example net-war between India–Pakistan, Israel–Pakistan etc

7.3.3 International Cyber Terrorist Attack:

The latest front is the war on cyber terrorism. The Internet and associated networks have been under attack from many sectors including hackers, disgruntled employees, financial fraud perpetrators, cyber criminals and now state-sponsored cyber terrorists. When international terrorist groups communicate each other through internet and through their own network to attack any nation then it is called International cyber terrorist attack.

7.3.4 Network to Send Terror Messages:

The cyber criminals started to use new technology to develop their own website, and network to send terror messages and to communicate within or between groups.

7.3.5 Digital Signature System:

A digital code was created that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgivable. There are a number of different encryption techniques to guarantee this level of security. They use e-mail, SMS, encryption program and digital signature system to communicate themselves keeping secrecy and confidentiality of their activities.

7.3.6 Flowing Worm:

Flowing “worm”, virus, Trojan horse to collapse government and people interest sites, network and computer is also one mode of cyber terrorism.

7.3.7 Cyber Theft:

Cyber Crime is a criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cyber Crime also includes non-monetary offences, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. Not only that, commission of unauthorized access, hacking/tampering source code, cyber theft etc which cause unpredictable fear are also modes of cyber terrorism. The list is not exhaustive rather increasing very fast.

7.4 Vulnerabilities of SCADA:

Supervisory Control and Data Acquisition (SCADA) systems are the computers that monitor and regulate the operations of most critical infrastructure industries (such as the companies that manage the power grid). These SCADA computers automatically monitor and adjust switching, manufacturing, and other process control activities, based on digitized feedback data gathered by sensors. These control systems are often placed in remote locations, are frequently unmanned, and are accessed only periodically by engineers or technical staff via telecommunications links. However, for more efficiency, these communication links are increasingly connected to corporate administrative local area networks, or directly to the Internet.

Some experts believe that the importance of SCADA systems for controlling the critical infrastructure may make them an attractive target for terrorists. Many SCADA systems also now operate using Commercial-Off-The-Shelf (COTS) software, which some observers believe are inadequately protected against a cyber attack. These SCADA systems are thought to remain persistently vulnerable to cyber attack because many organizations that operate them have not paid proper attention to these systems unique computer security needs.

The following example may serve to illustrate the possible vulnerability of control systems and highlight cyber security issues that could arise for infrastructure computers when SCADA controls are interconnected with office networks. In August 2003, the 'Slammer" Internet computer worm was able to corrupt for five hours the computer control systems at the Davis-Besse nuclear power plant located in Ohio (fortunately, the power plant was closed and off-line when the cyber attack occurred). The computer worm was able to successfully penetrate systems in the Davis-Besse power plant control room largely because the business network for its corporate offices was found to have multiple connections to the internet that bypassed the control room firewall.

Other observers, however, suggest that SCADA systems and the critical infrastructure are more robust and resilient than early theorists of cyber terror have stated, and that the infrastructure would likely recover rapidly from a cyber terrorism attack. They, cite, for example, that water system failures, power outages, air traffic disruptions, and other scenarios resembling possible cyber terrorism often occur as routine events, and rarely affect national security, even marginally. System failures due to storms routinely occur at the regional level, where service may often be denied to customers for hours or days. Technical experts who understand the systems would work to restore functions as quickly as possible. Cyber terrorists would need to attack multiple targets simultaneously for long periods of time to gradually create terror, achieve strategic goals, or to have any noticeable effects on national security.

An important area that is not fully understood concerns the unpredictable interactions between computer systems that operate the different US infrastructures. The concern is that numerous interdependencies (where downstream systems may rely on receiving good data through stable links with upstream computers) could possibly build to a cascade of effects that are unpredictable in how they might affect national security. For example, while the "Blaster" worm was disrupting Internet computers over several days in August 2003, some security experts suggest that slowness of communication links, caused by Blaster worm network congestion, may have contributed to the Eastern United States power blackout that occurred simultaneously on August 14. The computer worm could have degraded the performance of several communications links between data centres normally used to send warnings to other utility managers downstream on the power grid.

7.4.1 DOD uses Commercial-off-the-Shelf:

DOD uses Commercial-off-the-Shelf (COTS) hardware and software products in core information technology administrative functions, and also in the combat systems of all services, as for example, in the integrated warfare systems for nuclear aircraft carriers. DOD favours the use of COTS products in order to take advantage of technological innovation, product flexibility and standardization, and resulting contract cost-effectiveness. Nevertheless, DOD officials and others have stated that COTS products are lacking in security, and that strengthening the security of those products to meet military requirements may be too difficult and costly for most COTS vendors. To improve security, DOD Information Assurance practices require deploying several layers of additional protective measures around COTS military systems to make them more difficult for enemy cyber attackers to penetrate.

7.4.2 Expert Security:

However on two separate occasions in 2004, viruses reportedly infiltrated two top-secret computer systems at the Army Space and Missile Defence Command. It is not clear how the viruses penetrated the military systems, or what the effects were. Also, contrary to security policy requirements, the compromised computers reportedly lacked basic anti-virus software protection. Security experts have noted that no matter how much protection is given to computers, hackers are always creating new ways to defeat, those protective measures.

7.5 Success of Cyber Attacks:

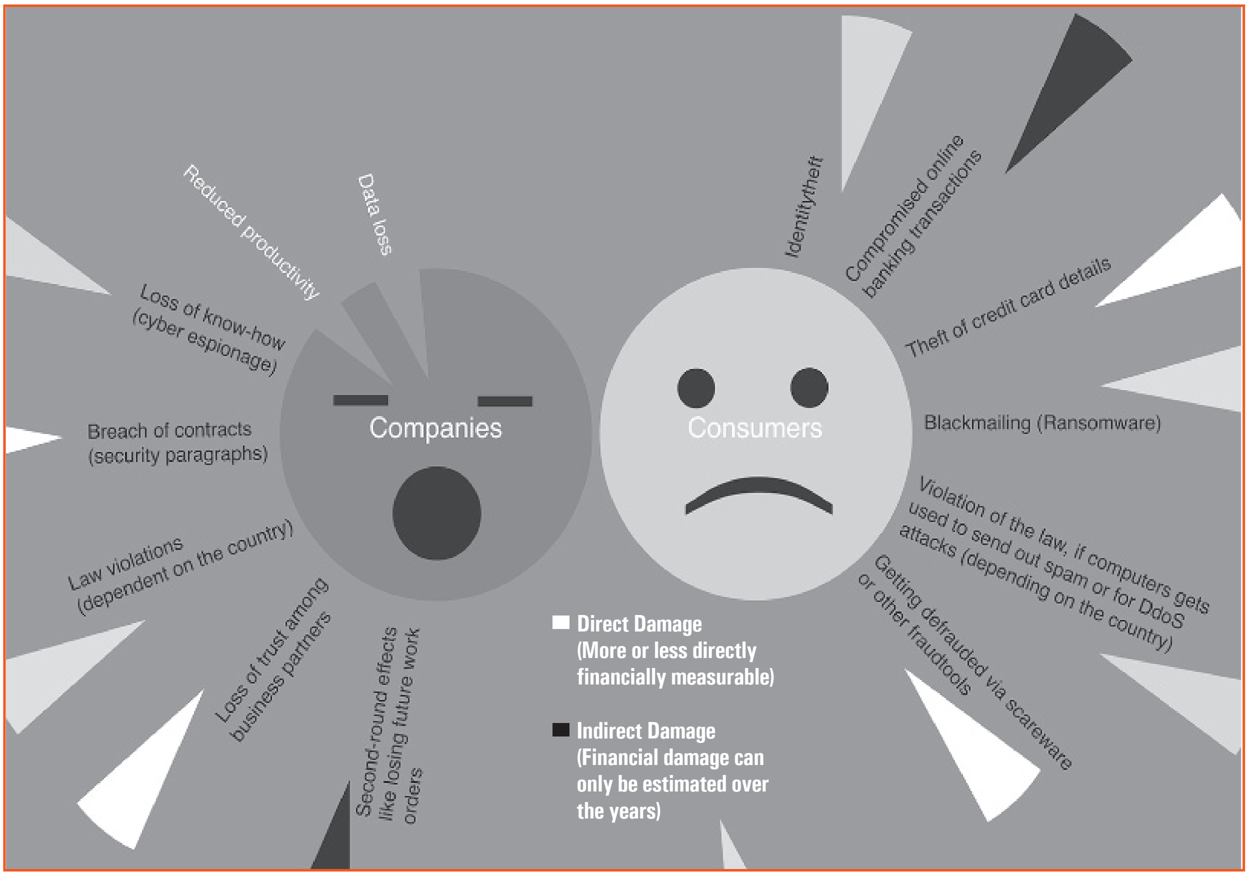

Reduced productivity
Data loss
Identitytheft
Compromised online banking transactions
Theft of credit card details
Loss of know-how (cyber espionage)
Companies
Consumers
Breach of contracts (security paragraphs)
Blackmailing (Ransomware)
Law violations (dependent on the country)
Violation of the law, if computers gets used to send out spam or for DDoS attacks (depending on the country)
Loss of trust among business partners
Second-round effects like losing future work orders
Getting defrauded via scareware or other fraudtools
□ Direct Damage (More or less directly financially measurable)
■ Indirect Damage (Financial damage can only be estimated over the years)

Fig. 7.2. Possible Consequences of Cyber Attacks

*"We must have friendship for all; we must be merciful toward those that are in misery; when people are happy, we ought to be happy; and to the wicked we must be indifferent. These attitudes will make the mind peaceful." - **Swami Vivekananda***

Networked computers with exposed vulnerabilities may be disrupted or taken over by a hacker, or by automated malicious code. Botnets opportunistically scan the Internet to find and infect computer systems that are poorly configured, or lack current software security patches. Compromised computers are taken over to become slaves in a "botnet", which can include thousands of compromised computers that are remotely controlled to collect sensitive information from each victim's PC, or to collectively attack as a swarm against other targeted computers.

Even computers that have updated software and the newest security patches may still be vulnerable to a type of cyber attack known as a "Zero-Day-Exploit". This may occur if a computer hacker discovers new software vulnerability and launches a malicious attack to infect computers before a security patch can he created by the software vendor and distributed to protect users. Zero-day vulnerabilities in increasingly complex software are regularly discovered by computer hackers. Recent news articles report that zero-day vulnerabilities are now available at online auctions, where buyers and sellers negotiate with timed bidding periods and minimum starting prices. This allows newly-discovered computer security vulnerabilities to be sold quickly to the highest bidder. Computer security expert Terri Forslof, of Tipping Point, has reportedly said that such practices will "increase the perceived value of vulnerabilities, and the good guys already have trouble competing with the money you can get on the black market."

7.5.1 The Insider Threat:

An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. The term can also apply to an outside person who poses as an employee or officer by obtaining false credentials. The cracker obtains access to the computer systems or networks of the enterprise, and then conducts activities intended to cause harm to the enterprise.

A major threat for organizations is the ease with which data can now be copied and carried outside using a variety of portable storage devices, such as small flash drives. Newer high-density memory stick technology reportedly allows installed computer applications to be run entirely from the flash drive. This means that the entire contents of a PC could possibly be copied to and stored on a small, easily portable, and easily concealed media device.

Employees with access to sensitive information systems can initiate threats in the form of malicious code inserted into software that is being developed either locally, or under offshore contracting arrangements. For example, in January 2003, 20 employees of subcontractors working in the United States at the Sikorsky Aircraft Corporation were arrested for possession of false identification used to obtain security access to facilities containing restricted and sensitive military technology. All of the defendants pleaded guilty and have been sentenced, except for one individual who was convicted at trial on April 19, 2004.

7.5.2 Persistence of Computer System Vulnerabilities:

Vulnerabilities in software and computer system configurations provide entry points for a cyber attack. Vulnerabilities persist largely as a result of poor security practices and procedures, inadequate resources devoted to staffing the security function may also contribute to poor

"Those who work at a thing heart and soul not only achieve success in it but through their absorption in that they also realize the supreme truth – Brahman. Those who work at a thing with their whole heart receive help from God."

security practices. Home PC users often have little or no training in best practices for effectively securing home networks and equipment.

7.5.3 Errors in New Software Products:

Fixing liability for the consequence of defective software is a very difficult matter for the law to deal with. Software has many functions and applications and is frequently dependent upon the operation of other technology to discharge its task correctly and efficiently. What steps can a legislature take in introducing product liability legislation for software to ensure that the legal terminology accurately defines the technical situation so as to categories software correctly and attach liability accordingly.

Vendors for Commercial-Off-the-Shelf software" (COTS) are often criticized for releasing new products with errors that create the computer system vulnerabilities. Richard Clarke, former White House Cyberspace advisor until 2003, has reportedly said that many commercial software products have poorly written, or poorly configured security features. In response to such criticism, the software industry reportedly has made new efforts to design products with architectures that are more secure. For example, Microsoft has created a special Security Response Centre and now works with DOD and with industry and government leaders to improve security features in its new products. However, many software industry representatives reportedly agree that no matter what investment is made to improve software security, there will continue to be vulnerabilities in future software because products are becoming increasingly more complex.

7.5.4 Inadequate Resources:

If the problem does not involve management control, it probably concerns resources. While senior management may agree that the TSP benefits are attractive, they may not have given your manager the resources to introduce it. In effect, they have told your intermediate manager that, since the TSP will save time and money, he or she should contain the cost and schedule impact within the current plan. While some managers may have sufficient flexibility to do this, few can. Generally, the only way to handle this problem is to convince the middle managers either to request added resources from senior management or to defer some other commitments. While the TSP is an attractive investment, it does not pay off instantly. The investment must be made at the beginning of each project, but the cost and schedule benefits come at the end.

Although software vendors periodically release fixes or upgrades to solve newly discovered security problems, an important software security patch might not get scheduled for installation on an organization's computers until several weeks or months after the patch is available. The job may be too time-consuming, too complex, or too low a priority for the system administration staff. With increased software complexity comes, the introduction of more vulnerabilities, so system maintenance is never-ending. Sometimes the security patch itself may disrupt the computer when installed, forcing the system administrator to take additional time to adjust the computer to accept the new patch. To avoid such disruption, a security patch may first require testing on a separate isolated network before it is distributed for installation on all other regular networked computers.

Because of such delays, the computer security patches installed in many organizations may lag considerably behind the current cyber threat situation. Whenever delays are allowed to persist in private organizations, in government agencies, or among PC users at home, computer vulnerabilities that are widely reported may remain unprotected, leaving networks open to possible attack for long periods of time.

7.5.5 Estonia, 2007:

Computer systems in Estonia—In the spring of 2007, government computer systems in Estonia experienced a sustained cyber attack that has been labelled by various observers as cyber warfare, or cyber terror, or Cyber Crime. On April 27, officials in Estonia moved a Soviet-era war memorial commemorating an unknown Russian who died fighting the Nazis. The move stirred emotions, and led to rioting by ethnic Russians, and the blockading of the Estonian Embassy in Moscow. The event also marked the beginning of a series of large and sustained Distributed Denial-Of-Service (DDOS) attacks launched against several Estonia national websites, including government ministries and the prime minister's Reform Party.

In the early days of the cyber attack, government websites that normally receive around 1,000 visits a day reportedly were receiving 2,000 visits every second. This caused the repeated shut down of some websites for several hours at a time or longer, according to Estonian officials. The attacks, which flooded computers and servers and blocked legitimate users, were described as crippling, owing to Estonia's high dependence on information technology, but limited resources for managing their infrastructure. Security experts say that the cyber attacks against Estonia were unusual because the rate of the packet attack was very high, and the series of attacks lasted weeks, rather than hour or days, which is more commonly seen for a denial of service attack. Eventually, NATO and the United States sent computer security experts to Estonia to help recover from the attacks, and to analyze the methods used and attempt to determine the source of the attacks.

This event can serve to illustrate how computer network technology has blurred the boundaries between crime, warfare, and terrorism. A persistent problem during and after any cyber attack is accurate identification of the attacker, by finding out whether it was sponsored by a nation, or was the independent work of a few unconnected individuals, or was initiated by a group to instil frustration and fear by damaging the computerized infrastructure and economy. The uncertainty of not knowing the initiator also affects the decision about whom should ultimately become a target for retaliation, and - whether the response should come from law enforcement or the military.

7.6 Some Other Examples:

Jeanson Ancheta, a 21-years old hacker and member of a group called the "Botmaster Underground", reportedly made more than $100,000 from different Internet Advertising companies who paid him to download specifically-designed malicious adware code onto more than 400,000 vulnerable PCs he had secretly infected and taken over. He also made tens of thousands more dollars renting his 400,000 unit "botnet herd" to other companies that used them to send out spam, viruses, and other malicious code on the Internet. In 2006, Ancheta was sentenced to five years in prison.

When crackers in Romania illegally gained access to the computers controlling the life support systems at an Antarctica research station, endangering the 58 scientists involved. However, the culprits were stopped before damage actually occurred. Mostly non-political acts of sabotage have caused financial and other damage, as in a case where a disgruntled employee caused the release of untreated sewage into water in Maroochy Shire, Australia, Computer viruses have degraded or shut down some non-essential systems in nuclear power plants, but this is not believed to have been a deliberate attack. (Note: it is also argued that this is actually not a case of cyber terrorism, but rather a case of Cyber Crime, as cyber terrorism requires a political motive and not a primary focus on monetary gain.)

In October, 2007, the website of Ukrainian President Viktor Yushchenko was attacked by hackers. A radical Russian nationalist youth group, the Eurasian Youth Movement, claimed responsibility.

In 1999 hackers attacked NATO computers. The computers flooded them with email and hit them with a Denial of Service (DOS). The hackers were protesting against the NATO bombings in Kosovo. Businesses, public organizations and academic institutions were bombarded with highly politicized emails containing viruses from other European countries.

7.7 Measuring Cyber Crime:

For example, according to a study by the Cooperative Association for Internet Data Analysis (CAIDA), on January 25, 2003, the SQL Slammer worm (also known as "Sapphire") automatically spread to infect more than 90% of vulnerable computers worldwide within 10 minutes of its release on the Internet, making it the fastest-spreading computer worm in history. As the study reports, the Slammer worm doubled in size every 8.5 seconds and achieved its full scanning rate (55 million scans per second) after about 3 minutes. It caused considerable harm through network outages which led to numerous cancelled airline flights and automated teller machine (ATM) failures.

Each year, the Computer Security Institute (CSI), with help from the FBI, conducts a survey of thousands of security practitioners from US corporations, government agencies, financial institutions, and universities. The CSI/FBI Computer Crime and Security Survey, published annually, is perhaps the most widely-used source of information about how often computer crime occurs and how expensive these crimes can be. The 2006 survey indicated that the average financial loss reported due to security breaches was $167,713 an 18% decrease from the previous year's average loss of $203,606.

However, some observers argue that the analyzes reported in the CSI/FBI survey may be questionable, because the survey methodology is not statistically valid. This is because the survey is limited only to CSI members, which reduces the likelihood that respondents are a representative sample of all security practitioners, or that their employers are representative of employers in general. In addition, the 2006 CSI/FBI survey points out that most companies are continuing to sweep security incidents under the rug.

With the apparent absence of statistically valid survey result concerning the financial costs of computer crime, and with an accompanying lack of clear data about the number and types of computer security incidents reported, it appears that there may be no valid way to currently understand the real scope and intensity of Cyber Crime. The growing use of botnets and sophisticated malicious code also suggests that the percentage of unreported Cyber Crime, plus the percentage undetected, may both be going up.

7.7.1 Problems Tracing Cyber Crime:

The challenge of identifying the source of attacks is complicated by the unwillingness of commercial enterprises to report attacks, owing to potential liability concerns. CERT/CC estimates that as much as 80% of all actual computer security incidents still remain unreported. Law enforcement officials concede they are making little progress in tracing the profits and finances of Cyber criminals. Online payment services, such as PayPal and E- Gold, enable criminals to launder their profits and exploit the shortcomings of international law enforcement. Recently, intermix Media was fined $7.5 million in penalties for distribution of spyware which silently captures personal information from user's PCs. However, some adware and spyware purveyors reportedly can still make millions of dollars per year in profits. Many companies who distribute spyware are difficult to pursue legally because they typically also offer some legitimate services. In many cases, the finances that back Cyber Crimes are so distributed they are hard for law enforcement to figure out.

7.7.2 Better Measurement of Cyber Crime Trends:

Experiences at CERT/CC show that statistical methods for measuring the volume and economic effects of cyber attacks may be questionable. Without sound statistical methods to accurately report the scope and effects of Cyber Crime, government and legal authorities will continue to have unreliable measures of the effectiveness of their policies and enforcement actions.

Figures from several computer security reports now used for measuring annual financial losses to US industry due to intrusions and Cyber Crime are believed by some observers to be limited in scope or possibly contain statistical bias. Is there a need for a more statistically reliable analysis of trends in computer security vulnerabilities and types of cyber attacks to more accurately show the costs and benefits for improving national cyber security? Congress may wish to encourage security experts to find more effective ways to collect data that will enable accurate analysis of trends for cyber attacks and Cyber Crime. Congress may also wish to encourage security researchers to find better ways to identify the initiators of cyber attacks.

7.8 Federal Efforts to Protect Computers:

The federal government has taken steps to improve its own computer security and to encourage the private sector to all adopt stronger computer security policies and practices to reduce infrastructure vulnerabilities. In 2002, the Federal Information Security Management

Act, (FISMA) was enacted, giving the Office of Management and Budget (OMB) responsibility for coordinating information security standards and guidelines developed by federal agencies. In 2003, the National Strategy to Secure Cyberspace was published by the Administration to encourage the private sector to improve computer security for the US Critical infrastructure through having federal agencies set an example for best security practices.

The National Cyber Security Division (NCSD), within the National Protection and Programs Directorate of the department of Homeland Security (DHS) oversees a Cyber Security Tracking. Analysis and Response Centre (CSTARC), tasked with conducting analysis of cyberspace threats and vulnerabilities, issuing alerts and warnings for cyber threats, improving information sharing, responding to major cyber security incidents, and aiding in national level recovery efforts. In addition, a new Cyber Warning and Information Network (CWIN) has begun operation in 50 locations, and serves as an early warning system for cyber attacks. The CWIN is engineered to be reliable and survivable, has no dependency on the internet or the Public Switched Network (PSN), and reportedly will not be affected if either the Internet or PSN suffer disruptions.

In January 2004, the NCSD also created the National Cyber Alert System (NCAS), a coordinated national cyber security system that distributes information to subscribers to help identify, analyze, and prioritize emerging vulnerabilities and cyber threats. NCAS is managed by the United States Computer Emergency Readiness Team (US-CERT), a partnership between NCSD and the private sector, and subscribers can sign up to receive notices from this new service by visiting the US-CERT website.

7.8.1 International Convention on Cyber Crime:

Cyber Crime is also a major international challenge, even though attitudes about what comprises a criminal act of computer wrongdoing still vary from country to country. However, the Convention on Cyber Crime was adopted in 2001 by the Council of Europe, a consultative assembly of 43 countries, based in Strasbourg. The convention, effective July 2004, is the first and only international treaty to deal with breaches of law ”over the internet or other information networks.” The Convention requires participating countries to update and harmonize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other illicit cyber activities.

Although the United States has signed and ratified the convention, it did not sign a separate protocol that contained provisions to criminalize xenophobia and racism on the Internet, which would raise constitutional issues in the United States. The separate protocol could be interpreted as requiring nations to imprison anyone guilty of insulting publicly, through a computer system certain groups of people based on characteristics such as race or ethnic origin, a requirement that could make it a crime to e-mail jokes about ethnic groups or question whether the Holocaust occurred. The Department of Justice has said that it would be unconstitutional for the Unites States to sign that additional protocol because of the First Amendment’s guarantee of freedom of expression. The Electronic Privacy Information Centre, in a June 2004 letter to the Foreign Relations Committee, objected to US ratification of the Convention, because it would “create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards.”

On August 3, 2006, the US Senate passed a resolution of ratification for the Convention. The United States will comply with the Convention based on existing US federal law; and no new implementing legislation is expected to be required. Legal analysts say that US negotiators succeeded in scrapping most objectionable provisions, thereby ensuring that the Convention tracks closely with existing US Laws.

7.8.2 DOD and Cyber Attack Response:

If a terrorist group were to use a Cyber Crime botnet to subvert computers in a third party country, such as China, to launch a cyber attack against the United States, the US response to the cyber attack must be carefully considered, in order to avoid retaliating against the wrong entity. Would the resulting effects of cyber weapons used by the United States be difficult to limit or control? Would a cyber attack response that could be attributed to the United States possibly encourage other extremists, or rogue nations, to start launching their own cyber attacks against the United States? Would an attempt by the US to increase surveillance of another entity via use of cyber espionage computer code be labelled as an unprovoked attack, even if directed against the computers belonging to a terrorist group? If a terrorist group should subsequently copy, or reverse-engineer a destructive US military cyber attack program, could it be used against other countries that are US. Allies, or even turned back to attack civilian computer systems in the United States? If the effects become widespread and severe, could the US use of cyber weapons exceed the customary rules of military conflict, or violate international laws.

Commercial electronics and communications equipment are now used extensively to support complex US weapons systems, and are possibly vulnerable to cyber attack. This situation is known to our potential adversaries. To what degree are military forces and national security threatened by computer security vulnerabilities that exist in commercial software systems; and how can the computer industry be encouraged to create new COTS products that are less vulnerable to cyber attack?

7.9 The Need to Improve Cyber-Security:

Department of Defence (DOD) officials have stated that, while the threat of cyber attack is “less likely” to appear than conventional physical attack, it could actually prove more damaging because it could involve disruptive technology that might generate unpredictable consequences that give an adversary unexpected advantages. The Homeland Security Presidential Directive 7 required that the Department of Homeland Security (DHS) coordinate efforts to protect the cyber security for the nation’s critical infrastructure. This resulted in two reports in 2005, titled “Interim National Infrastructure Protection Plan,” and “The National Plan for Research and Development in Support of Critical Infrastructure Protection,” where DHS provided a framework for identifying and prioritizing, and protecting each infrastructure sector.

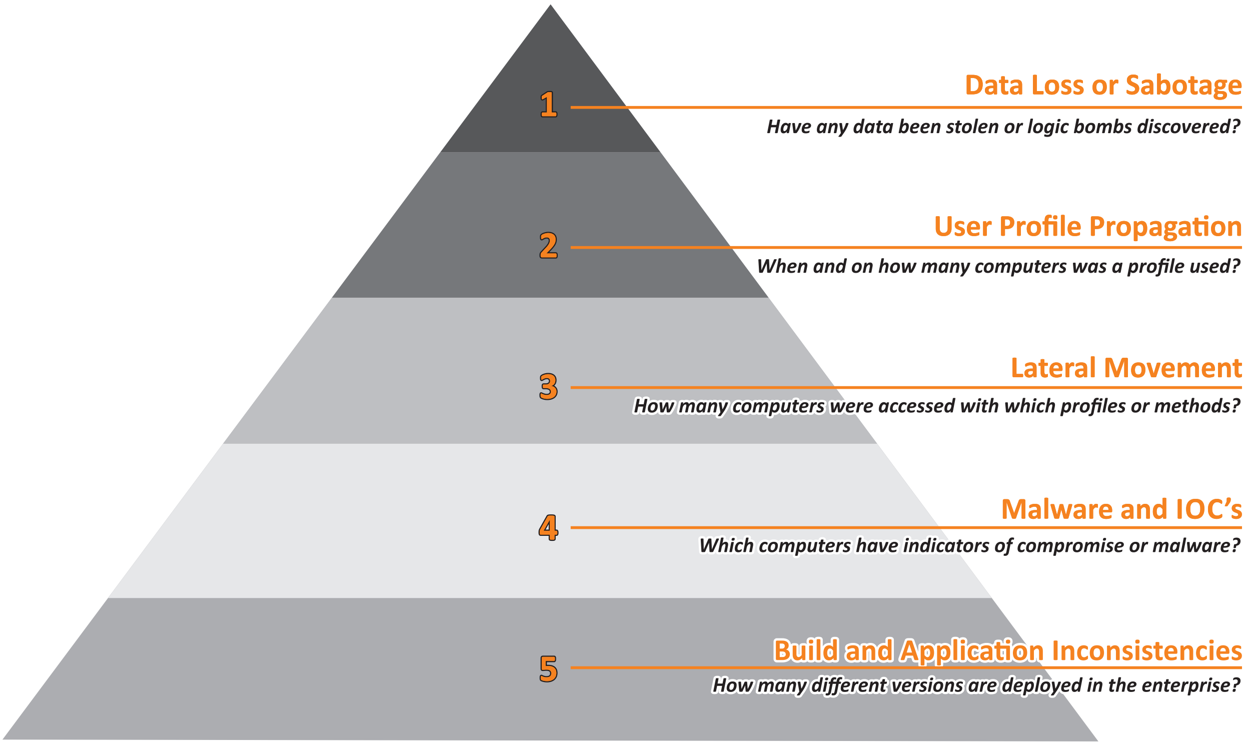

1
Data Loss or Sabotage
Have any data been stolen or logic bombs discovered?
2
User Profile Propagation
When and on how many computers was a profile used?
3
Lateral Movement
How many computers were accessed with which profiles or methods?
4
Malware and IOC's
Which computers have indicators of compromise or malware?
5
Build and Application Inconsistencies
How many different versions are deployed in the enterprise?

Fig. 7.3. Cyber Security impacts on Nation's Critical Infrastructure

However, some observer's question why, in light of the many such reports describing an urgent need to reduce cyber security vulnerabilities, there is not an apparent perceived sense of national urgency to close the gap between cyber security and the threat of cyber attack. For example, despite Federal Information Security Management Act of 2002 (FISMA), some experts argue that security remains of low priority, or is treated almost as an afterthought at some domestic federal agencies. In 2007, the Government Accountability Office issued a report, titled "Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain," which states that cyber security risks have actually increased for infrastructure control systems because of the persistence of interconnections with the internet, and continued open availability of detailed information on the technology and configuration of the control systems. The report states that no overall strategy yet exist to coordinate activities to improve computer security across federal agencies and the private sector, which owns the critical infrastructure. Some observers argue that, as businesses gradually strengthen their security policies for headquarters and administrative systems, the remote systems that control critical infrastructure and manufacturing may soon be seen as easier targets of opportunity for Cyber Crime.

Cyber Crime is obviously one of the risks of doing business in the age of the internet, but observers argue that many decision-makers may currently view it as a low-probability threat. Some researchers suggest that the numerous past reports describing the need to improve cyber security have not been compelling enough to make the case for dramatic and urgent action by decision-makers. Others suggest that even though relevant information is available, future possibilities are still discounted, which reduces the apparent need for present-day action. In addition, the costs of current inaction are not borne by the current decision-makers. These researchers argue that IT vendors must be willing to regard security as a product attribute that is coequal with performance and cost; IT researchers must be willing to value cyber security research as much as they value research for high performance or cost-effective computing; and, finally, IT purchasers must be willing to incur present-day costs in order to obtain future benefits.

7.9.1 Growth in Technical Capabilities of Terrorists:

Terrorism is both a subjective and a pejorative term. This being so, difficulties emerge in attempting to find a definition of terrorism that can be classified as universal. The key problem with defining terrorism is that it is ultimately a moral judgment shaped by social and political contexts and so, definitions will vary depending on these contexts. But how can we have a "global" war on terrorism when there will never be unanimity over exactly who the terrorists are? It has of course been argued that those who are labelled terrorists have been driven to act in the way that they do because it is the only means left to them to tackle "injustice." The argument is that they act out of desperation, and while their actions can be perceived by some as reprehensible there will always be others who support them.

Seized computers belonging to AL Qaeda. Indicate its members are becoming more familiar with hacker tools and services that are available over the Internet. Could terrorist groups find it advantageous to hire a Cyber Crime botnet tailored to attack specific targets, possibly including the civilian critical infrastructure of Western nations? Could Cyber Crime botnets, used strategically, provide a useful way for extremists to amplify the effects of a conventional terrorist attack using bombs?

As computer-literate youth increasingly join the ranks of terrorist groups, will cyber terrorism likely become increasingly more mainstream in the future? Will a computer-literate leader bring increased awareness of the advantages of an attack on information systems, or be more receptive to suggestions from other, newer computer-literate members? Once a new tactic has won widespread media attention, will it likely motivate other rival terrorist groups to follow along the new pathway?

7.9.2 Incentives for the National Strategy to Secure Cyberspace:

Does the National strategy to secure Cyberspace present clear incentives for achieving security objectives? Suggestions to increase incentives may include requiring that all software procured for federal agencies be certified under the "common criteria" testing program, which is now the requirement for the procurement of military software. However, industry observers point out that the software certification process is lengthy and may interfere with innovation and competitiveness in the global software market.

Should the National Strategy to Secure Cyberspace rely on voluntary action on the part of private firms, home users, universities, and government agencies to keep their networks secure, or is there a need for possible regulation to ensure best security practices? Has public response to improve computer security been slow partly because there are no regulations currently imposed?

Would regulation to improve computer security interfere with innovation and possibly harm US competitiveness in technology markets? Two of the former cyber security advisers to the president have differing views : Howard Schmidt has stated that market forces, rather than the government, should determine how product technology should evolve for better cyber security; however, Richard Clarke has stated that the IT industry has done little on its own to improve security of its own systems and products.

7.10 Future Attractiveness of Critical Infrastructure Systems:

There has yet been no published evidence showing a widespread focus by Cyber criminals on attacking the control systems that operate the US civilian critical infrastructure. Disabling infrastructure controls for communications, electrical distribution or other infrastructure systems, is often described as a likely scenario to amplify the effects of a simultaneous conventional terrorist attack involving explosives.

However, in 2006, at a security discussion in Williamsburg, Virginia, a government analyst reportedly stated that criminal extortion schemes may have already occurred, where cyber attackers have exploited control system vulnerabilities for economic gain. And, in December 2006, malicious software that automatically scans for control system vulnerabilities reportedly was made available on the internet for use by Cyber criminals. This scanner software reportedly can enable individuals with little knowledge about infrastructure control systems to locate a SCADA computer connected to the Internet, and quickly identify its security vulnerabilities.

The Idaho National Laboratory is tasked to study and report on technology risks associated with infrastructure control systems. Past studies have shown that many, if not most, automated control systems are connected to the Internet, or connected to corporate administrative systems that are connected to the Internet, and are currently vulnerable to a cyber attack. And, because many of these infrastructures SCADA systems were not originally designed with security as a priority, in many cases, new security controls cannot now be easily implemented to reduce the known security vulnerabilities. Following past trends, where hackers and Cyber criminals have taken advantage of easy vulnerabilities, some analysts now predict that we may gradually see new instances where Cyber criminals exploit vulnerabilities in critical infrastructure control systems.

7.11 Awareness through Education:

7.11.1 Improving Security of Commercial Software:

The main concern is that because free and open source software (FOSS) is built by communities of developers with the source code publically available, access is also open to hackers and malicious users. As a result, there could be the assumption that FOSS is less secure than proprietary applications. Another concern is that the FOSS community might be slower to issue critical software patches as vulnerabilities emerge. FOSS proponents claim these anxieties are unfounded and open source can match shrink-wrapped and proprietary software for security and, in some cases, offer greater security.

Some security experts emphasize that if systems administrators received the necessary training for keeping their computer configurations secure, then computer security would greatly improve for the US critical infrastructure. However, should software product vendors be required to create higher quality software products that are more secure and that need fewer patches? Could software vendors possibly increase the level of security for their products by rethinking the design, or by adding more test procedures during product development?

7.11.2 Education and Awareness of Cyber Threats:

Prior to the first Cyber Security Awareness Month in October 2004, discussions on national security had very little to do with technology. However, due to the increasing threat of domestic and international cyber attacks on America's public and private infrastructure after 9/11, a need arose to promote cyber security beyond simple computer password protection. Sponsored by the Department of Homeland Security National Cyber Security Division (NCSD) and the non-profit National Cyber Security Alliance, Cyber Security Awareness Month is a time to promote security awareness among all participants in the digital sphere. Of course, the concept is much more advanced than merely password protecting computers and mobile devices. A recent article in Computer Weekly reported that cyber attacks, whether like recent ones by the Syrian Digital Army or various groups of computer hackers, will rise significantly in the next decade.

Ultimately, reducing the threat to national security from Cyber Crime depends on a strong commitment by government and the private sector to follow best management practices that help improve computer security. Numerous government reports already exist that describe the threat of Cyber Crime and make recommendations for management practices to improve cyber security.

A 2004 survey done by the National Cyber Security alliance and AOL showed that most home PC users do not have adequate protection against hackers, do not have updated anti-virus software protection, and are confused about the protections they are supposed to use and how to use them. How can computer security training be made available to all computer users that will keep them aware of constantly changing computer security threats, and that will encourage them to follow proper security procedures?

7.11.3 Coordination between Private Sector and Government:

Coordination is extremely important in order to resolve any potential conflicts between the economic and environmental goals and to formulate holistic policies. In order to achieve this goal, countries such as Nepal and the Philippines have already created advisory councils to the planning authority, such as the Environment Protection Council and PCSD respectively, with multi-sectoral representation from government as well as from NGOs and the private sector to ensure that different interests and viewpoints are considered before a given policy is designed to accomplish national goals.

What can be done to improve sharing of information between federal government, local governments, and the private sector to improve computer security? Effective cyber security requires sharing of relevant information about threats, vulnerabilities, and exploits. How can the private sector obtain information from the government on specific threats which the government now considers classified, but which may help the private sector protect against cyber attack? And, how can the government obtain specific information from private industry about the number of successful computer intrusions, when companies resist reporting because they want to avoid publicity and guard their trade secrets? Should Cyber Crime information voluntarily shared with the federal government about successful intrusions be shielded from disclosure through Freedom of Information Act requests?

How can the United States better coordinate security policies and international law to gain the cooperation of other nations to better protect against a cyber attack? Pursuit of hackers may involve a trace back through networks requiring the cooperation of many internet service providers located in several different nations. Pursuit is made increasingly complex if one or more of the nations involved has a legal policy or political ideology that conflicts with that of the United States.

Thirty-eight countries, including the United States, participate in the Council of Europe's Convention on Cyber Crime, which seeks to combat Cyber Crime by harmonizing national laws, improving investigative abilities, and boosting international cooperation. However, how effective will the Convention without participation of other countries where Cyber criminals now operate freely?

Intents behind Cyber Terrorism:

- Political protestors may have rented the services of Cyber criminals, possibly a large network of infected PCs, called a 'botnet,' to help disrupt the computer systems of the Estonian government.
- Cyber attacks from individuals and countries targeting economic, political, and military Organizations.
- Cyber criminals have reportedly made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where profitable illegal activities are used to support terrorist groups;
- Trends in Cyber Crime are described, showing how malicious Internet websites and other Cyber Crimes such as identity theft are linked to conventional terrorist activity.

7.12 Web War against India:

A general perception has been created in the West, from continuous reports of cyber attacks originating in China that most Cyber Crime and hacking originate from China. The US, Belgium, France and Russia have stated that China is attempting to control the cyberspace 'offensively' through the cyber operations of the Chinese People's Liberation Army. According to the US, in September 2007, the Chinese military was planning a cyber attack targeting a Pentagon computer system in the office of US Defence Secretary Robert Gates. According to reports, China has internally set a deadline of 2050 for China to be able to stop any military attack through cyber warfare. Moreover, hackers have been mobilized into Unions and Red Alliances with alleged 'official backing.' At the same time, China has protected itself by a firewall known as the 'Great Red Firewall.'

Revolution did not necessarily involve sanguinary strife. It was not a cult of bomb and pistol.
- Shahid Bhaghat Singh

Several years ago, the Belgian justice minister claimed that attacks against the Belgian Federal Government originated from China and were likely to have been approved by the Chinese government. In the words of expert Mr. Brahma Chellaney, 'The Chinese are opening a new front of asymmetrical warfare for India.' 'On the one side we have Pakistan saying terrorist are non-state actors and on the other, the Chinese are saying hackers are non-state actors.' However, as pointed out by Mr. Chellaney, it is not clear why a non-state actor would attack Indian government, security and defence targets.

Since 2006, China has reportedly been waging daily cyber attacks on Indian computer systems, both private and governmental. The Chinese are constantly scanning and mapping India's official networks which not only gives them access of the content but will enable them to disable the networks during a conflict between the two countries.

In 2008, the main attacks attributed to China were an attack on NIC (National Informatics Centre), which was aimed at the National Security Council, and on the Ministry of External Affairs (MEA). In April 2008, Indian government officials stated that the computer network of the MEA had been broken into allegedly by Chinese hackers. The hackers allegedly broke into the internal communications network of the MEA and accessed the emails bearing information on policies and decision matters across the Ministry's offices in India and in their foreign missions. Similar allegations had been made against China back in June 2007 which were denied.

In September 2008, the newspaper DNA reported that suspected Chinese hackers had breached cyber security at high levels in the government of India as well with many cabinet ministers complaining that their emails accounts had been hacked.

On February 21, 2009, the Information Warfare Monitor reported that 10 websites belonging to various ministries and departments of the government of India had been hacked by attackers suspected to be from China. According to reports in the newspaper DNA, a senior official of IT Ministry, Government of India, stated, 'Low to medium intensity cyber intrusions into web servers maintained by the Indian government have been reported.

In March 2009, attempts were reportedly made at hacking into the computers of Indian Embassies and spyware was found on computers. Subsequently, the MEA and Indian Embassies has reportedly issued strict rules on email usage by bureaucrats and imposed rules requiring them to frequently change passwords and use emails only for routine communications. The MEA has also commenced periodic security reviews of all MEA computers to check for spyware and other computer threats.

On December 15, 2009, computers in the Indian Prime Minister's Office (PMO) and the MEA in New Delhi were hacked by planting a Trojan virus' from a mail purportedly sent from China. The Trojan virus allowed the attackers to access and delete the personal Gmail accounts of Government officials. The attack was discovered by Google engineers in Silicon Valley, North California who then reportedly mounted a secret counter-offensive attack to detect the Chinese intruders who had accessed the government's private Gmail accounts. The investigators were able to verify the internet protocol addresses and the Media Access Control (MAC) addresses, which are unique identification numbers, of the hackers and confirmed they, originated in China.

According to a report in *The New York Times,* a team from Google remotely accessed a computer in Taiwan that they suspected to be the source of the attack and then found that the attack had been planned on the Chinese mainland. The hidden virus had come in an email and was embedded in an Adobe Acrobat attachment which had breached both Gmail's and other networks' security. Both the Indian investigators and Google engineers were of the view that the data stolen through the Trojan could only be of use to a government. On the same date, December 15, 2009, various US companies, including Google, reported cyber attacks from China although China has denied any role in the attacks.

The December 15, 2009 attack was reported by National Security Advisor, M.K. Narayanan to *The Times*, London who was quoted as saying, 'This is not the first instance of an attempt to hack into our computers.' Concerned about the attack, the Indian government sent a team of intelligence officials to audit the security standards of the systems and computers in key Indian missions around the world.

In April 2010, the Army CERT issued a high alert to all military formations and installations to guard against 'focused large scale cyber attacks' that are being planned on 'internet facing' government organizations, prominent brands and corporate groups. According to the Army CERT alert, effective measures must be taken to protect networks from data thefts, distributed denial of service attacks, paralyzing computer viruses and the like mainly from Chinese hackers. Some military establishments, including the Defence Services Staff College at Wellington had apparently even refrained from using computers directly connected to the internet when the alert was sounded.

An April 2010 report on cyber attacks on India, entitled 'Shadows in the Cloud: Investigating Cyber Espionage 2.0' by John Mark-off and David Barboza, two Canadian researchers at the Munk School of Global Affairs at the University of Toronto, John (hereinafter the 'Shadows Report') explains how an India-focused spy ring based in Chengdu, Peoples Republic of China (PRC), used social networking sites such as Twitter, Google Groups, Blogspot, blog.com, Baidu Blogs and Yahoo! Mail to take over control of computers in India after they had been infected by viruses or other malware. The shocking revelation of the Shadows Report was that, based on geographic location, the vast majority of the compromised computers were in India. The Shadows Report analyzes how the attackers 'leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the Peoples Republic of China.' The attackers obtained documents from the Indian government marked 'secret', 'restricted' and 'confidential' as discussed in detail below.

An earlier investigation by the authors of the Shadows Report, John Mark-off and David Barboza, resulted in a Report entitled 'Tracking Ghost net: Investigating a Cyber Espionage Network' (hereinafter Tracking Ghost net) which focused on allegations of Chinese cyber espionage against the Tibetan community. For the Tracking Ghost net investigation, the researchers undertook field investigations in India, Europe and North America. The Tracking Ghost net report documented 1,295 compromised computers spread across 103 countries, 30% of which were identified as being 'high-value' targets, including ministries of foreign affairs, embassies, international organizations, news organizations and a computer located at NATO headquarters. The Tracking Ghost net report found that Indian government related entities, both in India and throughout the world has been compromised, including computers at the Indian embassies in Belgium, Serbia, Germany, Italy, Kuwait, the US, Zimbabwe and the High Commissions of India in Cyprus and the UK. However, the Tracking Ghost net report did not find enough evidence to implicate the Chinese government.

In March 2010, the Canadian and American computer security researchers undertook a second investigation which involved monitoring a spying operation for eight months, and observed while the intruders stole classified and restricted documents from the highest levels of the Indian Defence Ministry. As discussed above, the Shadows investigators found that the India-focused spy ring used social networking service providers such as twitter, Google and others to infect email or social networking with malware which, in turn, allowed the compromised computer to receive more sophisticated malware through attachments. The master servers in China monitored the infiltration of computers in order to transfer documents from personal details to missile analysis to safe drop zones.

The Shadows investigators found that the hackers had stolen classified documents from the Indian government and reports from Indian military analysts and corporations as well as documents from agencies of the United Nations and other governments. The documents stolen were marked with 'Secret,' 'Restricted' and 'Confidential' notices. In addition to encrypted diplomatic correspondence, two documents were marked 'Secret,' six as 'Restricted' and five as 'Confidential.' The stolen documents according to the report, contain sensitive information taken from a member of the National Security Council Secretariat concerning secret assessments of India's security situation in the states of Assam, Manipur, Nagaland and Tripura as well as concerning the Naxalites and Maoists. The stolen documents also contained confidential information taken from Indian embassies regarding India's international relations with and assessments of activities in West Africa, Russia/ Commonwealth of Independent States and the Middle East as well as visa applications, passport office circulars and diplomatic correspondence.

The Shadows investigators also found evidence that Indian Embassy computers at a number of missions, including the Embassies in Kabul, Moscow and Dubai, United Arab Emirates, and at the High Commission of India in Abuja, Nigeria had been compromised. Computers used by the Indian Military Engineering Services in Calcutta, Bangalore and Jalandhar; the 21 Mountain Artillery Brigade in Assam and three air force bases were also reportedly compromised, including the Air Force Station at Race Course Road opposite the Prime Minister's residence. According to the Shadows Report, computers at the Army Institute of Technology at Pune and Military

College of Electronics and Mechanical Engineering at Secunderabad were also compromised.

According to the Shadows Report, the spies also stole information regarding several Indian missile systems. According to the Shadows Report, the spies also took documents relating to network centricity (SP's Land Force 2008) and network-centric warfare along with documents detailing plans for intelligence fusion and technologies for monitoring and analyzing network data (Defence Research and Development Organization 2009). The Shadows Report also lists a number of institutions in India as having been affected by the attacks, including the National Security Council Secretariat, Military Engineer Services and other military educational institutions as well as several companies.

After uncovering a series of e-mail addresses, the investigators traced the attacks to hackers based in Chengdu, China where a large number of Tibetans are based. The researchers believe that the hackers may have been affiliated with the prestigious University of Electronic Science and Technology located in Chengdu. The Shadows Report also examined the extent to which the attackers are linked to the Chinese government. According to the Shadows Report, one possibility is that the state authorizes private persons to perform attacks against enemies of the state — a view which is supported by the finding that there is no direct government control over the groups of hackers in the PRC. According to the Shadows Report, information independently obtained by the Chinese hacker community is likely to find its way to elements within the Chinese state.

On March 24, 2010, the Shadows investigators contacted intelligence officials in India on March 24, 2010 and informed them of the spy ring they had been tracking. They requested and were given instructions on how to dispose of the classified and restricted documents. However, the China-based cyber spy network targetting the Indian military and the consequent alert by the Army authorities may be only the beginning. Subsequent investigations have revealed a fully dedicated India-specific espionage system aimed at business, diplomatic, strategic and academic interests.

The Chinese are known to use mainly three weapons against Indian networks: BOTS, key loggers and mapping of networks (each of these types of Cyber Crimes is discussed in detail in the next section of this chapter). The Chinese are reportedly experts in setting up BOTS which is a parasite program embedded in a network (known as BOTNETS) which hijacks the network and makes other computers act as per its instructions. The controlled computers are known as 'zombies' and are a key tool in cyber warfare. Therefore, at a selected time, the controller of the BOTNETS will command the zombies at their will. In other words, there are networks in India which are controlled by China. Therefore, it is not surprising that a cyber attack on government websites operating out of the Prime Minister's Office on March 21, 2010 was traced to an Indian IP address linked to the ISP Videsh Sanchar Nigam Ltd. (VSNL).

Key loggers is software that scans computers and their processes and data the moment a person strikes a key on the keyboard. This information is immediately carried over to an external controller so they know even when you change your password. Mapping or scanning networks is done as a preliminary step to cyber warfare tactics.

7.12.1 Indian Government Response:

The Government of India's response to the Shadows Report was essentially to acknowledge the hacking attempts but maintain that the hackers were never successful. The Ministry of Defence stated that it was 'studying the report' which had 'lot of grey areas.' However, the Ministry of External Affairs reportedly considered cyber security cooperation with the Munk School of Global Affairs at the University of Tornonto.

The Ministry of Communications & Information Technology has issued security guidelines to all ministries and government departments asking them to set up 24x7 cyber control rooms, implement information security best practices deploy information security experts and formulate their own information security policies. The National Crisis Management Committee (NCMC) headed by the Cabinet Secretary also monitors all national-level cyber crises. The Government of India is reportedly developing a full-fledged Crisis Management Plan for countering cyber attacks such as the recent attack on Indian Embassies.

The Crisis Management Plan calls for each central administrative department under each critical sector to set up 24-hour control rooms which will get activated immediately after a crisis situation is reported and also prepare detailed contingency plans. Each department is required to screen and do background checks of all employees engaged in implementing and monitoring cyber security and crisis management plans including contractors and third party users. Each employee is to be checked for satisfactory character references, accuracy of CVs, claimed academic and professional qualifications, credit checks, criminal record checks and independent identity checks in the form of passport or similar documents. Organizations have also been directed to implement periodic IT security risk assessments, back up of files critical to mission accomplishment, security awareness training of personnel and periodic testing and evaluation of technical security measures.

Indian diplomats have reportedly been prohibited from: logging into social networking sites such as Facebook, Orkut and Ibibo, downloading peer-to-peer music; sharing photos through Flicker and Picasa, writing a blog; and using G-mail, Yahoo! or Hotmail for official communications.

In a written reply to a question raised in the Lok Sabha on July 27, 2010, the Department of Information Technology (DIT) stated that it has initiated a major program on cyber forensics specifically focused on development of cyber forensic tools, setting up of infrastructure for investigation and training of law enforcement and judicial offices in use of cyber forensic tools, to collect and analyze the digital evidence. Further, DIT has set up cyber forensic training labs at CBI and Kerala Police for skill upgradation in the area of Cyber Crime investigations and have also sponsored projects in the North Eastern States to establish cyber forensic training facilities at the state police organizations. Besides, Indian Computer Emergency Response Team (CERT -In) under DIT has been set up for creating awareness about cyber security. It performs both pro-active and reactive roles.

Nevertheless, India is considered to be slow in developing corrective measures in the event of a web-attack and has failed to come up with an aggressive strategy to counter the attacks. Cyber warfare is not yet a major component of India's security doctrine.

7.13 Cyber Terrorism in India:

Cyber terrorism in India is not a new concept. However, for long concepts like cyber warfare, cyber terrorism, etc were not taken seriously by Indian government. Naturally, cyber security in India also could not flourish. The cyber security capabilities of India also could not develop in such circumstances.

Techno legal experts of India have been warning against growing incidences of cyber attacks, Cyber Crimes, cyber espionages, etc. against India. Further, the fact that critical infrastructure protection in India is needed has also been reiterated from time to time. The truth is that cyber attacks are affecting Indian critical infrastructure and we are not even aware of the same.

Ethnic Tamil guerrillas attacked Srilanka embassies with thousands of e-mail. The message read as follows "we are the internet Black Tigers and we are doing this to disrupt your communications this is an off-shoot of the Liberation Tigers of Tamil Eelam (LTTE).

CASE STUDY ▶ ***45: Cyber Terrorism over Indian Parliament:*** In the year 2001, 13th December attack on the Indian Parliament was with help of information technology. Accused committed cyber forgery and made gate pass official logo of Ministry of Home Affairs and other information with layout of Indian Parliament, Police found out a laptop computer from main accused Md. Afzal and S. Hussein Guru and also found out that they did it through Pakistani Internet Service Provider. They controlled the identity and e-mail system of Indian Army.

CASE STUDY ▶ ***46: July 11, 2006 Terrorist Attack:*** Information technology becomes easy tool beyond—imagination on the hand of terrorists. World is witness of measurable disastrous terrorists attack on India on July 11, 2006. In the era of communication convergence terrorists are using computers, wireless and mobiles i.e. computers to communicate with each other's and to simplify their activities with quick action. Therefore, on the same day almost at the same time serial bomb blasts were their target; at first Srinagar and then Mumbai. Electronic media has flashed breaking news on July 12, 2006 that behind frequent blasts in Srinagar and Mumbai, the culprits were Lashkar e taiba, Al Qaeda, Simi etc as suspected by Maharashtra Police. Maharashtra Police found out explosives just before one month of Mumbai blast from Aurangabad and Nasik. Police also found out one suspected resident of Malegaon at Maharashtra who left India for Pakistan just after explosion.

CASE STUDY ▶ ***47: Cyber Terrorism—Cyber War:*** Net-war or cyber-war and cyber terrorism is not only prevalent in USA, UK, Australia, France etc but also in Bangladesh, Pakistan and in India. Now-a-days most of Indian department sifes are defaced and attacked by Pakistani hackers and terrorist groups. Information and Communications Technology (ICT) are in great use by terrorists in Bangladesh, Pakistan and India too. In the

I always believed that my silence on several topics will be an advantage in the long run. ***- Lala Lajpat Rai*** year 2000, within 4 months almost 132 Indian websites were defaced and the number was increased in the year 2001 by 161. The hackers group named "Silver Lords" hacked about 23 Indian websites within 6 days demanding independence for Kashmir. One Pakistani website called "Global net.pk" was also hacked by "Silver Lords". Most of the Indian websites are hacked and defaced by Paisani hackers e.g. G-Force Pakistan, Harkat-ul-mos.etc They are generally popular for anti-Indian hacking in 2001 after Pokhran II tests. Western hackers attacked on Bhaba Atomic Research Centre to steal nuclear test data. Another Anti-Indian hackers group is Fantabulous Defacers. The Pakistani hackers group was detected by one Indian ethical hacker Mr. Anand Khare known as Dr. Neruker.

CASE STUDY ***48: Indian Legislation:*** The Indian Parliament passed the Information Technology Act 2000 following the United Nations Model Law, 1997 but does not define the term "cyber terrorism", "Cyber Crimes" etc However, Section 66 prohibits cyber hacking and prescribes punishment and Section 65 prohibits tampering source code and prescribes punishments. The terrorist activities are prohibited by several laws in India several times e.g. the Preventive Detention Act. The Prevention of Terrorism Act 2000 repealed the Terrorist and Disruptive Activities Act (TADA) etc The Prevention of Terrorism Act 2000 was passed for 3 years though it was mentioned that penalty, forfeiture, punishment and proceedings under the Act will continue to be operational after its expiry. This Act prohibits terrorist and disaster related activates, using any property, weapons or harbouring for terrorist activities. The Prevention of Terrorism Ordinance (POTO) 2001 (No. 9 of 2001, dated 24.10.2001) was made for the prevention of terrorist and related activities. Investigators became empowered to extract information from any one they suspect and failure to reveal information was punishable with up to 3 years imprisonment. Even without knowledge, holding a property derived from terrorist or acquired through terrorists fund was punishable offence. Not only that if a person was found in unauthorized possession of arms in a special or notified area, he would presumed for being linked with terrorist activities under POTO.

CASE STUDY ***49: Ayodhya Incident:*** Indian Police found mobile phone link with Unani doctor Irfan Khan and terrorist of Ayodhya incidents with Amin @ Zuber. Police found out, only after 1 hour of Ayodhya incident through mobile called ID and detected that Gazi Misbah-ud-Din the operational chief of Kashmir's biggest indigenous militant has link with this incident. The Short Message Service (SMS) conversation was as such: "Hello, this is Gazi Note it down, we have not done it."

CASE STUDY ***50: Cyber Terror in Kolkata:*** One encrypted message was stored by Mr. S. Kundus cyber cafe's Technician on December, 2002 at Kolkata that one computer file was found called "PAKI-G. BABA 0241" in the D-drive. Out of curiosity he opened it and found that terrorising message with misspelling of some famous buildings in Kolkata e.g. "Ratters Building", "Bikash Bhawan" "2nd Hogly Bridge" etc with possible dates and times of terrorist attack. But due to extra alert and security measures of Kolkata Police no incident occurred. Similar message was found in webpage before Durga Puja 2005 and people

"All love is expansion, all selfishness is contraction. Love is therefore the only law of life. He who loves lives, he who is selfish is dying. Therefore love for love's sake, because it is law of life, just as you breathe to live. " - ***Swami Vivekananda***

in Kolkata were alerted by Government. Aftab Ansaris network from Dubai and New Delhi to attack American Centre at Kolkata was cyber terrorism.

CASE STUDY ▶ ***51: Cyber Terrorism by Hackers:*** On May 2001 the Indian Government and e-business sectors raised voice to act against anti-Indian hacking especially against Pakistani hackers and Government constituted a force on cyber security. Therefore, unlocking the source codes of Pakistani websites was taken as way to prevent and control cyber terrorism e.g., June 2000 defacement of Indian website for showing disrespect to the Indian flag, 27th June, 2001 defacement of www.knitwear.com.etc Thus, Indian Pakistan cyber was going on every moment.

CASE STUDY ▶ ***52: Cyber Terrorism in India Link to the UK Blast:*** Al Qaeda linked terrorist and accused of London blast Md. Afozol of 29 years old was sentenced to 7 years rigorous imprisonment by the Prevention of Terrorist Activities Court, in India, Special Judge A.P. Bhargale awarded the sentence on 22nd July, 2005 on the charge of conspiracy with his uncle in the UK named M.M. Nizam to cause terror and destruction in England, Australia and the USA by hijacking planes, crashing vital locations etc He was also charged with "forgery for producing fake certificates of a Pune College to get admission in a pilot training institution in Mumbai and abroad". The Court also directed to bring his Uncle into India, Police seized international credit cards, global roaming mobile phone, and passport etc from him. Al Qaeda influenced India origin H.R. Aswat made numerous calls to the terrorist and was arrested from Islamabad though he went out of the UK just few hours before London blast on tube train and bus on 7th July, 2005. At the time of his arrest he was armed with and wore a belt of explosives and had £17,000 and British passport. He is cousin of terrorist who died in 2002 Gujarat riots in India.

7.14 Prevention and Control of Cyber Terrorism in India:

The convergence of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called 'cyberspace'. This cyberspace has become a platform for a galaxy of human activities which converge on the internet. The cyberspace has, in fact, become the most happening place today. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. There is hardly any human activity that is not touched by the internet. Therefore, Internet has something to offer to everybody and in the process it only increases and never diminishes. The 'cyber manthan' has bestowed many gifts to humanity but they come with unexpected pitfalls. It has become a place to do all sort of activities which are prohibited by law. It is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy and corporate espionage, to name a few.

Nowadays most of the terrorist groups have their own websites or information way (I-way); for example, one of the Al Qaeda based websites in Arabic language is http://www.mojahedoon.net which has link with Osama Bin Laden. Information and Communication Technology are very much used by terrorists in India whether for attack against the nation or only with intent to attack Jammu and Kashmir (J&K).

Case Study ***53: Cyber Terrorism in Jammu and Kashmir:*** In Jammu and Kashmir the website and network are used by terrorists for communication between senior commanders in the Kashmir valley and control station. Between Kashmir Valley and Doda-Udhampur-Rajauri regions and North – South Pir Panjal range there were Lines of Site (LOS) to provide network facilities. Earlier terrorists used to use High Frequency Radio Network as means of communication. In April – May 2003 three cellular phones and one satellite phone were recovered in Surankat area by army operation. In India, terrorists are also users of BSNL network along with STD and ISD facilities to connect with Pakistan and other countries.

Case Study ***54: Use of Telephone and Mobile by Terrorists:*** Since 1999 onwards use of mobile phones and electronic mail with internet use is increasing day by day among terrorist groups as convenient means to communicate, control and monitor their groups. To avoid detections and investigations terrorists frequently use different cyber cafes. They are using remote controlled Improvised Explosive Devices to cause death and destruction. They are communicating with other terrorist groups worldwide through internet.

A charge sheet was filed in the year 2002 against Abu Salem Ansari and others by Delhi Police. Mr. Ashok Gupta filed a complaint reporting that over telephone one person as claimed by himself as Abu Salem Ansari called him to call back either of three numbers as mentioned by him, these are as follows:

1. 00971507367248 (roaming),
2. 0060193034859 (roaming) and
3. 00871665341860 (satellite phone) in Dubai.

The alleged accused caused threat to the complainant and his family. His son also received another call from same mobile phone. The Police found that total six mobile phones in Delhi were connected with Abu Salem's group and other landline phones of Pawan Kumar Mittal @ Raja Bhai and Sajjan Kumar Soni @ Babu Bhai of Chandni Chowk were also found having connection with Abu Salem Ansari. Through these phones the accused made threat to complainant, a shooter of Abu Salem Ansari, Mr. Asharaf @ Babloo also made potential threat. Thereafter they were trying to change SIM card of mobile phone, Police traced them with the help of International Mobile Equipment Identity (IMEI) which was specific to a hand set and was transmitted over the air prior to setting up the call.

Case Study ***55: The Information Technology Act 2000 with 2006 Amendment Bill and Terrorism:*** Following the United Nations' MODEL LAW 1997, the Computer Fraud and Abuse Act 1986 of the USA, the Computer Misuse Act 1990 and the Data Protection Act 1984 of the UK, and International Convention and treaties, the Indian Parliament enacted and passed the Information Technology Act 2000 which was amended twice in the years 2006 and 2008 with the object to evolve world standard security measures to regulate cyber world and to prevent and control Cyber Crimes but not yet enforced.

In India Cyber Crimes are dealt with under our traditional legal system and we do not have special court to deal with the matter. Till now Cyber Crimes are dealt with following the

Criminal Procedure Code, the Indian Penal Code and the Information Technology Act 2000. Though the Information Technology Act 2000 provides for Information Technology (Appellate) Tribunal and accordingly Rules 2000 were made but till date these are not implemented. We do not have any Legislation specially dealing with Cyber Crimes like Malaysia has. However, NASSCOM President Kiran Karnik also expressed his view towards establishment of Fast Track Court to deal with cyber terrorism.

The term 'Cyber Crime' is not defined under the present Act. Possible definition of Cyber Crime may be as follows: "Human conducts which are prohibited by State under criminal law and which are related to Information Technology as target or as tools." But to have a specific concept of Cyber Crime, the definition of crime itself has to be specific. We can define crime as human conduct, which are prohibited by the State through criminal law.

CASE STUDY *56: Propensity of Terrorists for Hacking:* In India terrorists are motivated for hacking and defacements of websites. Anti-Indian Crew (AIC), Pakistani Hackers' Club (PHC), G-Force Pakistan, Pro-Pak Hackers are terrorists groups who are working with Al Qaeda and Bin Laden. Some of these groups are represented by Dr. Neruker who hacked the website of Zee News.

Dr. Neruker also attacked the website of Indian Cyber Crime cell at Mumbai with co-accused Mr. Mahesh Mhatre and posted objectionable material on that website abusing the police administration. The police arrested them but they were released on bail. After release they repeated Cyber Crimes commission i.e., credit card theft affecting several American and other victims though they were employed by Mumbai police and CBI for technical assistance to prevent and control Cyber Crimes. They were recognized as ethical hackers.

In the year 2001 Mr. Manoj Singhania and Mr. Prakash Yadav of Chhattisgarh were arrested on the charge of attempt to hack into the computers of the State Bank of India. They sent e-mails in the name of Microsoft and Videsh Sanchar Nigam Containing speed.exe file which had capacity to send back e-mails to the accused with passwords and other information of the users.

One Anti-India Crew posted in internet was as follows: "... Message is for the innocent people being killed in Jammu Kashmir and you know what the reason behind all this killing is? PIECE OF LAND. I will keep on defacing and passing out this word around the world proving our point. How lame Indians are and their network security is even worse!" On 10th January 2001 Mr. R.K. Ragavan the Director of CBI said to Info Sec News that a number of cases of hacking of Indian internet sites have been traced to Pakistan but it would be difficult to nail them. In the year 2005, July there were 635 incidents of breaking Indian internet sites.

The Pakistani hackers group was founded by one Indian hacker known as Dr. Neruker whose actual name is Mr. Anand Khare. He said that the aim of the Pakistani hackers group was to hack for the injustice going around the Globe, especially with [sic] Muslims. In May 2001, Indian Government and e-business sectors raised voice to act against anti-Indian hacking especially Pakistani hackers. To achieve this goal Government constituted a force on cyber security.

Taking shelter in the dead is death itself, and only taking all the risk of life to the fullest extent is living.
*- **Sir Rabindranath Tagore***

According to Dewang Mehtia, former President of NASSCOM about 635 Indian websites were hacked during the year 2000. The awareness on e-security was very poor in India. Companies here were spending only 0.8% of their information technology spending annually as against the world average of 5.5%.

CASE STUDY ***57: Encryption of Message:*** In December 2002, in Kolkata one encrypted message was stored by Mr. S. Kundu's Cyber Cafe which contains fears of a terror strike in the city. The owner of the Cyber Cafe said that one computer file was found by his technician. The file name was <"PAKI_G.BABA0241" in the D-drive. Out of curiosity he opened the file. It contains misspelling of some famous buildings in Kolkata e.g. Raiters Building, Bikash Bhawan, Fharakk Bridge, 2nd Hoogly Bridge with possible date and time of attack. Thereafter, the Kolkata Police were alerted and due to extra security measures no incident occurred subsequently.

CASE STUDY ***58: Some New Tools Used by Terrorists:*** New technology is also producing several new weapons e.g., E-Bomb, High Energy Radio Frequency (HERF) guns, High Altitude Nuclear Explosions, High Power Microwave bombs, Nano-devices, Micro-electromechanical devices coupled with robotics which allow terrorists access to security system and high radiation explosions which cause lose of Low Earth Orbit satellites even within a month. These weapons are used by terrorists worldwide. More than 50 websites provide recipe for making RDX bombs to net users worldwide. Not only that, electronic mail system for communication is more reliable way for terrorists; they also have their own websites to express and publish their views. They often use encrypted data to transfer huge sums of money and data. They use denial of service attack, sabotage, computer espionage, cryptography and other forms of unauthorized use, misuse and abuse of new multimedia technology.

Three school boys made a hoax call and disturbed the train scheduled to Sealdah from North Bengal on 26th February night. They were Class XI students of McWilliam High School. They made a phone call from their mobile on the way from private tuition to home in evening taking advantage of unlimited free calls offer. As that was the last day of the offer they made 22 calls within one hour threatening about blast, loot of house, calls to assistant of MLA representing themselves as extremists from Jharkhand and so forth. Immediately with the cooperation of people and assistant of MLA the Calcutta police control room in Lalbazar traced the accused. Due to these terror calls the train was stopped at several destination and checked, though nothing was found out.

Police arrested those boys but said "we grilled the boys for three hours. They had committed the nuisance unintentionally. We have cautioned them against doing this in future. They were absolutely free thereafter on the ground that they were young. However, headmaster of the school said he will not allow students to carry mobile phone within the campus".

CASE STUDY ***59: Terrorists of Ayodhya Incident June 2005:*** On 23rd July 2005, Indian Police found mobile phone link with Unani doctor Irfan Khan and terrorist of Ayodhya incidents. In this connection one of the terrorist was identified as Amin@zuber native village man of Dr. Khan. During this search police also unearthed two militants in Akbarpur who rented a room, where the police found out torn hand sketch of Ayodhya incident and 4th July newspapers. Just after one hour of Ayodhya Temple attack it was found out on Tuesday through a caller identifying mobile phone system that Gazi Misbah-ud-Din was the operational Chief of Kashmir's biggest indigenous militant outfit. The mobile phone conversation as claimed was "Hello, this is Gazi. Note it down we have not done it. In fact, we condemn this attack. It is a handiwork of Hindu extremists and right wing political parties. For, no one but they have benefited from this attack". It was not only Gazi who picks up BSNL or Airtel phone rather all militants use these for terrorist activities. Another militant in Kashmir Valley Al-Nasreen called up from his mobile phone and informed the local news agency about the responsibility of 11th May blast at Jawahar Nagar causing one dead and 45 injured. Not only that one spokesman for the pro-Pakistani outfit said over mobile phone "by detonating the car bomb we have exposed the security lapses in Srinagar and we will continue these activities until India withdraws its troops from Kashmir".

On 11th July 2005, Indian Prime Minister Dr. Manmohan Singh on his return to New Delhi from the G-8 summit said "This (London blasts) is a vivid demonstration that terrorism is a global phenomenon. We have suffered from this scourge for nearly 20–25 years. The blasts are a demonstration that all of us will have to work together to evolve a collective strategy to free the world from this scourge".

CASE STUDY ▶ ***60: Indian Link with Al Qaeda:*** An Al Qaeda linked group claimed responsibility of suicide bomb and attempted bombing at London. Suspected Al Qaeda linked terrorist and accused of London blast Mohammed Afzal of 29 years old was sentenced to 7 years rigorous imprisonment by Prevention of Terrorist Activities Court's special Judge AP Bhangale on 22nd July 2005. He was charged on conspiracy with his uncle in the UK named Mubarak Musalman Nizam to cause terror and destruction in England, Australia and the USA by hijacking planes, crashing them into vital locations etc He was also charged with forgery for producing fake Higher Secondary mark sheets and certificates of a Pune College to get admission in Pilot training institutes in Mumbai and abroad. Therefore, the court gave directions to take steps to bring his uncle into India. Police seized international credit cards, global roaming mobile phone, passport which contains immigration seals of several Countries from the accused.

British Security Agencies found network links between London Pakistani suicide bombers and Al Qaeda influenced Haroon Rashid Aswat the son of Indians who immigrated to the UK in the year 1950. He allegedly made numerous calls to the terrorists. He was arrested from Sargodha 90 miles from Islamabad. He went out of the UK just few hours before the blasts of London tube train and bus network on 7th July 2005. At the time of arrest he was armed with and wore a belt of explosives and had £17,000 with British passport. According to Federal Bureau of Investigation, he had link with Al Qaeda and once travelled in an Air India flight to the United States of America for Jihadi Training Camp in Oregon. He is the cousin of terrorists who died in the year 2002 Gujarat riots in India. London blasts were the example of cyber terrorism in which we can find Indian link with Al Qaeda. Al Qaeda used internet, network to effectuate their works easily and quickly. For example, Al Qaeda group Abu Hafs Al-Masri Brigades has claimed in an internet statement that in the year 2004 train bombings in Madrid, in the year 2003 attacks on Istanbul, through internet attack to cause ultimate threat to Iraq, the US, the UK and other countries were part of their operation so that those countries might change their policy towards Islam and Muslims. Also they had stated in internet the deadline to other countries to stop running behind the USA Even on September 2005 Osama Bin Laden threatened India through internet to attack big shopping Mall and places. PTI reported that 15th August 2005 date was declared by terrorists through new information technology that there may be terrorist attack on temples, Airports, Government places by 'Jangri'. Therefore Government published security announcement.

Lal Quila from where Prime Minister would deliver speech was to be specially secured and initiatives were taken with about 1000 security forces. Government had to prohibit airlines or helicopter around Lal Quila till end of 15th August's program and also announced about the cancellation of Lal Quila trains. Lashkar-i-Taiba, Jaish e mohammed, Babbar khalsa, ULFA and others from North East for bombardment, air attack and suicidal attack were planned by terrorists by using new technology. Kolkata, Mumbai, Ahmadabad and other cities in India including Metro Trains were possible important places which were terrorised and for which special security forces were appointed.

CASE STUDY ▶ ***61: Use of Trojan Horse and Viruses by Terrorists:*** In the same week, it was breaking news in India on 16th July 2005 that a Trojan virus posted as an online CNN news letter containing exclusive video footage of the terrorist attack with the words "TERROR HITS LONDON" and invites recipients to see video shots attachments. The moment recipients started downloading the program, it started copying the users system and access the e-mail servers to send spam and junk mails. Anti-virus companies called it 'Don Bomb', 'Spam SPM', 'Spexsta' etc The spam mail contains the story of either death of Osama Bin Laden or Saddam Hussein and other data. More than 53,000 computers were affected. In June 2005, just one month before a Trojan also flowed information about suicide of Michael Jackson and Arnold Schwarzenegger which infected more than 1000 personal computers. The 'Don Bomb' was out just after an hour of 7th July London blasts.

7.15 International Initiatives to Prevent and Control of Cyber Terrorism:

Cyber terrorism is now one of the most complex international and global problems. There is great need international and global co-operation and co-ordination worldwide. The United Nations and European Union always played and are playing significant role to prevent and control conflicting global problems. The International Ministerial Conference on Global Information Networks 1997 was held in Bonn with the aim to bring world together for the protection of net users and to evolve world standard security measures. With the same aim the Council of Justice and Home affairs also came forward to establish worldwide practical co-operation. Not only that P8 Senior level group on the Transnational Organized Crime had undertaken several program to identify and prosecute computer related Crimes. In the year 1997, December G-8 Conference was held at the FBI headquarter of the Justice Ministers of the G-8 Countries. The Conference report released for collaboration of nations on following:

i. Assignment of adequate number of properly trained and equipped law enforcement personnel to investigate Cyber Crime;

ii. To improve preventive and controlling measures;

iii. Where extradition is impossible, to prosecute offender in the country where he was found;

iv. To keep key evidence on computer etc

The European Committee on Crime Problem and Committee of Experts on Crime in cyber-space adopted a draft convention on Cyber Crimes on 22nd December, 2000 for the prevention and control of Cyber Crimes and international co-operation. The convention also adopted necessary measures to deter activities against confidentiality, integrity and availability of computer system, networks and data of every nation state.

On 11th September, 2001 attack on World Trade Centre (WTC) was nothing but cyber terrorism. Terrorist's unauthorized access over the network of one airline and hijacked two airlines and resulted crashing of those airlines into WTC twin towers and Pentagon. On the other hand on 12th September, 2001 the United Nations General Assembly and Security Council condemned terrorists attack on the USA and asked for international co-operation to combat terrorist activities. On 18th September, 2001, the United Nation Security Council called on the Taliban to hand over Osama-bin-laden who established several websites and Al-quaida network based on Alzazeera etc On 28th September, 2001 the council established few measures to combat terrorism. After incident of 7th July, 2005 London, G-8 leaders asked for international co-operation to improve controlling measure on radioactive and telecommunication source worldwide.

Notes :

अध्याय 8
Chapter 8
Evidentiary Value of Videoconferencing

Notes :

8.1 General:

Conducting a conference between two or more participants at different sites by using computer networks to transmit audio and video data. For example, a point-to-point (two-person) Videoconferencing system works much like a video telephone. Each participant has a video camera, microphone, and speakers mounted on his or her computer. As the two participants speak to one another, their voices are carried over the network and delivered to the other's speakers, and whatever images appear in front of the video camera appear in a window on the other participant's monitor.

Videoconferencing is a cost effective method of facilitating live, interactive communication across different geographical locations. Videoconferencing systems used to be found in the largest multi-national corporations, due to their high expense, but in recent years the technology has been more widely adopted. Videoconferencing can be used for a variety of purposes, including:

- Meetings with colleagues working away from the office.
- Project collaboration between staff working at multiple sites.
- Participate in presentations from different geographical locations.
- Collaboration with different research groups.
- Can give access to locations which may not normally be possible (due to health and safety, security, or audience size limitations).
- Videoconferencing cannot replace face to face meetings completely, and there are some limitations to videoconferencing as a format. However, the benefits the format gives in terms of reduced travel time and easier collaborative working are hard to ignore. Videoconferencing actually encompasses a range of technologies used in a wide range of situations, often it is not just video and audio that is transmitted, but also data, allowing collaborative working though shared applications.

Videoconferencing may be:

- **One-to-one meetings** also known as point to point communications, usually involving full two-way audio and video.
- **One-to-many** involving full audio and video broadcast from the main site, where other sites may be able to send audio. For example in a lecture situation, students could ask questions.
- **Many-to-many** known as multi-point communication, provides audio and video between more than two sites. With most multi-point systems only one site in a conference can be seen at time, with switching between sites either controlled manually or voice activated (i.e., the loudest site is on screen).

Physically, the most common scenarios of Videoconferencing are:

- **Desktop Videoconferencing** usually a small camera is located on top of the PC or workstation monitor. The actual video is usually displayed in a small window, and shared applications, such as a shared whiteboard are often used.
- **Studio-based systems** a studio is specially equipped for Videoconferencing. This will normally include one or more cameras, microphones, one or more large monitors, and possibly other equipment such as an overhead camera for document viewing. Usually used for more formal meetings.

In practice a 'studio' may not be a dedicated room, but a standard seminar room with portable equipment that can be set up when required.

8.2 Meaning of "Videoconferencing":

A simple definition of Videoconferencing is "A televise telephone class whereby two or more parties can speak in real time and also see each other in real time. It necessarily involves a camera, one or more monitors, and microphones for each participant, audio speakers and other necessary equipment."

8.3 Criticisms of Videoconferencing:

Videoconferencing, especially current desktop Videoconferencing systems, have received significant criticism. Certain criticism has been directed at the difficulty in configuring and operating the systems, the quality of their output, and limitations related to the use and compatibility of systems of different brands.

Another criticism holds that pervasive Videoconferencing will end up increasing, not decreasing, the total amount of time allotted to meetings. Another flaw that has been pointed out is the fact that there cannot be any eye-to-eye contact because a person cannot simultaneously look directly into a camera and the screen.

However, the biggest concern in India would be that a witness in a video conference from an unsecured location could be under threat without the knowledge of the Court. For e.g., a witness deposing before a camera could have a gun pointed at his head from a distance and this would not show on the camera thus hampering the quality of evidence. Other activities around the witness may also be unseen by thus Court this gravely affecting the reliability of the testimony rendered

8.4 Videoconferencing Methods:

In order to further understand the concept of Videoconferencing the methods in which Videoconferencing may be conducted may be considered.

8.4.1 Videophone:

Videophone, also called video telephone, device that simultaneously transmits and receives both audio and video signals over telephone lines. In addition to the two-way speech transmission traditionally associated with the telephone, for many years there has been an interest in transmitting two-way video signals over telephone circuits in order to facilitate communication between two parties. Two-way video communication systems employ a videophone at each end. The videophone incorporates a personal video camera and display, a microphone and speaker, and a data - conversion device. The data - conversion device permits transmission of video over telephone circuits through the use of two components: a compression/expansion circuit, which reduces the amount of information contained in the video signal, and a modem, which translates the digital video signal to the analog telephone line format. "Videophones", i.e. telephones capable of sending and receiving atleast some type of a video image, were first introduced at the 1964 New York World's Fair with the "Picture Phone" These devices have not been very successful in India both because of high price and low quality.

8.4.2 Build a Centralized, in House Facility:

Videoconferencing has traditionally involved "an elaborate, expensive facility similar to a professional television production studio. Further, expensive high-bandwidth telephone lines, or satellite hookups were required. Today, in-house facilities can be built somewhat more affordably. Few large firms in India have full fledged Videoconferencing rooms with proper equipment. Certain Courts across the country also have dedicated video conference halls, e.g. Bangalore Criminal Court.

8.4.3 Desktop Videoconferencing Capabilities:

Imagine being able to meet face-to-face with remote colleagues, partners, and customers, without leaving your desk. Polycom Real Presence Desktop Solutions deliver easy-to-use HD Videoconferencing, voice, and content collaboration to individuals at all levels of the organization. This mode of Videoconferencing is probably the most common and most accessible to a small attorney and his witness. With the advent of technology and drop in prices, it is extremely affordable to video conference between two individuals at a preliminary level. In fact it is one of the most common means of communication amongst people.

8.5 Present Legal Scenario:

In the current legal system, evidence is collected under the provisions of the Indian Evidence Act and the Code of Criminal Procedure (hereinafter Cr. PC). Sections 230–234 of the Code of Criminal Procedure provide a Judge with the power to record evidence and compel appearance of witness in criminal cases. Section 273 of the Cr PC has been interpreted to provide for examination of witness via videoconferencing. Sections 30 – 34 of the Code of Civil Procedure provide the Court with the power to compel appearance of witness and recording of evidence in civil cases. Per se there is no express provision in the Indian Legal System which permits Videoconferencing and recording of testimony via Videoconferencing. However, there have been various case laws which permit the same.

8.6 Videoconferencing — Utility:

The unmet psychological needs of rural cancer patients are numerous. Tele psychology is a novel and feasible option that may provide cost-savings and help overcome inequalities in access to specialists. This is the first known study of psychological treatment for people with cancer delivered entirely via videoconferencing. We hypothesized that a tele psychology service would improve rural cancer patients' anxiety and depression levels and quality of life, and would be an acceptable, satisfactory, and practical mode of service delivery. Twenty-five cancer patients attended an average of three sessions with a clinical psychologist providing brief cognitive-behavioural therapy. Questionnaires were completed at pre post, and 1-month follow-up.

Affordably connect to multiple remote locations

Save money on travel expenses

Work more efficiencly among multiple locations

Connect easily internationally

Have compelling and rich conversations with clients

Fig. 8.1. Video Conferencing Benefits

Examination of witness where he resides far away or is physically inaccessible. Where the witness is unable to attend proceedings due to his ill health. Where there arise security concerns as to procuring the attendance of a witness or an accused.

"Anything that brings spiritual, mental, or physical weakness, touch it not with the toes of your feet."

8.7 Videoconferencing and its Evidentiary Value:

The case of Praful Desai decided the law in reference to Videoconferencing and its evidentiary value; it was subsequently referred to in the case of Sakshi v. Union of India. The facts in the case of Praful Desai were that, the complainant's wife was suffering from the terminal cancer. It was the case of the prosecution that the complainant's wife was examined by Dr. Ernest Greenberg of Sloan Kettering Memorial Hospital. New York, USA, who opined that she was inoperable and should be treated only with medication Thereafter the complainant and his wife consulted the respondent (Dr.Praful Desai), who was a consulting surgeon practising for the last 40 years. In spite of being made aware of Dr. Greenberg's opinion the respondent suggested surgery to remove the uterus. It was the case of the prosecution that the complainant and his wife agreed to the operation on the condition that it would be performed by the respondent. It was the case of the prosecution that on 22nd December 1987. Dr. A.K. Mukherjee operated on the complainant's wife when the stomach was opened ascetic fluids oozed out of the abdomen. Dr. A.K. Mukherjee contacted the respondent who advised closing up the stomach. Dr. A.K. Mukherjee accordingly closed the stomach and this resulted in intestinal fistula. Prosecution contended that whenever the complainant's wife ate or drank the same would come out of the wound. The complainant's wife required 20/25 dressings a day for more than 3-1/2 months in the hospital and thereafter till her death. The complainant's wife suffered terrible physical torture and mental agony and it was contended that the respondent did not once examine the complainant's wife after the operation.

A complaint by the complainant under Section 338 read with Sections 109 and 114 of the Indian Penal Code was registered against the respondent and Dr. A.K. Mukherjee. Process was issued by the Metropolitan Magistrate, 23rd Court, Esplanade, Mumbai. The respondent challenged the issue of process and carried the challenge right up to the Supreme Court. The Special Leave Petitions filed by the respondent was dismissed by the Supreme Court on 8th July, 1996 and the respondent was directed to face trial.

On 29th June, 1998 the prosecution made an application to examine Dr. Greenberg through Videoconferencing. The trial Court allowed that application on 16th August 1999. The respondent challenged that order in the High Court. The High Court allowed the criminal application filed by the respondent from which the respondent's appealed to the Supreme Court.

The question before the Supreme Court was with regard to the evidentiary value of Videoconferencing and whether it was within the due process of law. It was contended that Section 273 of Cr PC does not provide for the taking of evidence by Videoconferencing. Emphasis was laid on the words "Except as otherwise provided" in Section 273 and it was submitted that unless there is an express provision to the contrary, the procedure laid down in Section 273 has to be followed as it is mandatory. It was submitted that Section 273 mandates that evidence "shall be taken in the presence of the accused" and Videoconferencing did not place the witness in the presence of the accused.

The Hon'ble Supreme Court held that Section 273 mandated constructive presence and physical presence was not a must and in addition the meaning of evidence included both oral, documentary and electronic records. This meant that evidence in criminal matters could also be in the form of electronic records and the State could proceed to examine Dr. Guttenberg via Videoconferencing.

अध्याय 9
Chapter 9
Internet

Notes :

9.1 Concept of Internet:

The Internet is a global collection of computer networks that are linked together by devices called routers and use a common set of protocols for data transmission known as TCP/IP (transmission control protocol/Internet protocol). The primary purpose of the Internet is to facilitate the sharing of information. There are many different tools used on the Internet to make this possible. Some of the more common tools include email, list servs, newsgroups, telnet, gopher, FTP, and the World Wide Web. Probably the most popular of all Internet tools is the World Wide Web.

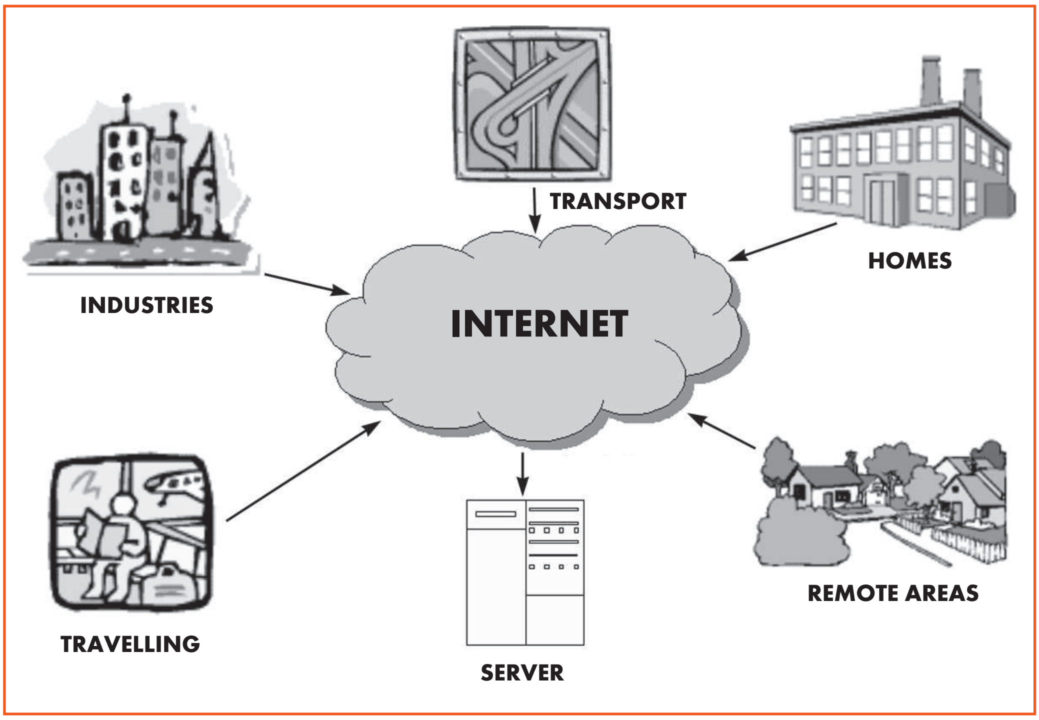


Fig. 9.1. Concept of Internet

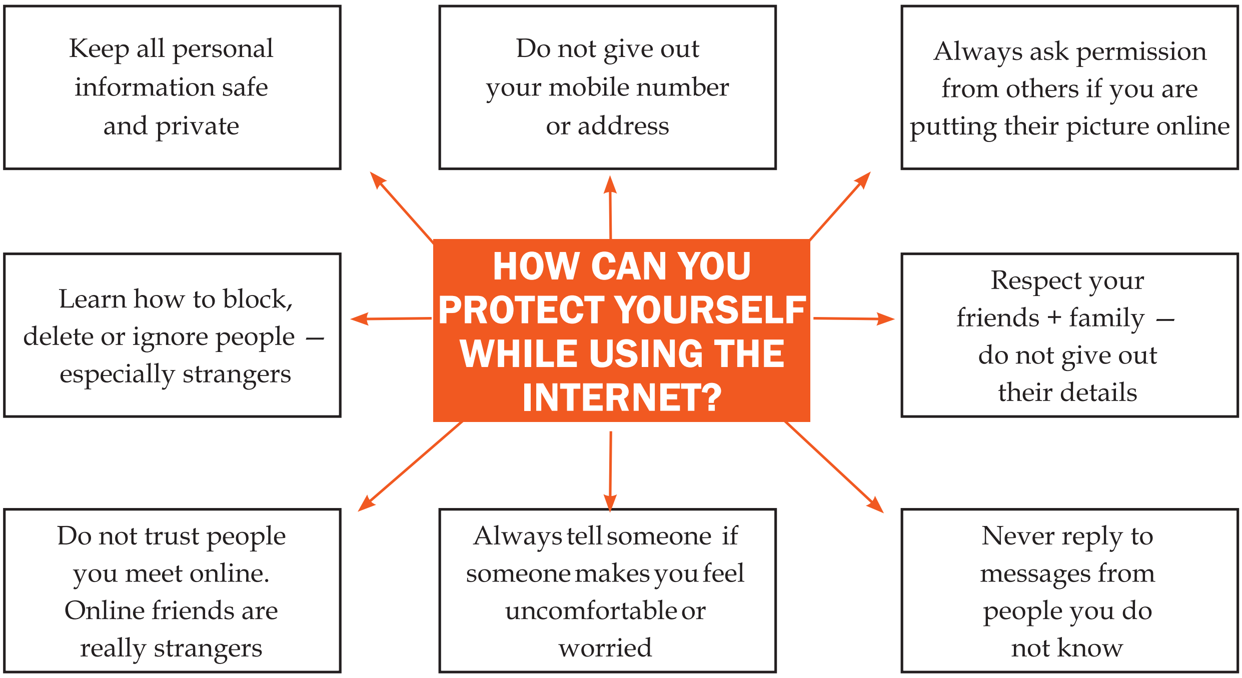
By the turn of the century, information, including access to the Internet, will be the basis for personal, economic, and political advancement. The popular name for the Internet is the information superhighway. Whether you want to find the latest financial news, browse through library catalogs, exchange information with colleagues, or join in a lively political debate, the Internet is the tool that will take you beyond telephones, faxes, and isolated computers to a burgeoning networked information frontier. The Internet supplements the traditional tools you use to gather information, Data Graphics, News and correspond with other people. Used skilfully, the Internet shrinks the world and brings information, expertise, and knowledge on nearly every subject imaginable straight to your computer.

What is the Internet?

The Internet links are computer networks all over the world so that users can share resources and communicate with each other. Some computers have direct access to all the facilities on the Internet such as the universities and other computers, e.g. privately-owned ones, have indirect links through a commercial service provider, who offers some or all of the Internet facilities. In order to be connected to Internet, you must go through service suppliers. Many options are offered with monthly rates. Depending on the option chosen, access time may vary.

The Internet is what we call a meta network, that is, a network of networks that spans the globe. It's impossible to give an exact count of the number of networks or users that comprise the Internet, but it is easily in the thousands and millions respectively. The Internet employs a set of standardized protocols which allow for the sharing of resources among different kinds of computers that communicate with each other on the network. These standards, sometimes referred to as the Internet Protocol Suite, are the rules that developers adhere to when creating new functions for the Internet. The Internet is also what we call a distributed system; there are no central archives. Technically, no one runs the Internet. Rather, the Internet is made up of thousands of smaller networks. The Internet thrives and develops as its many users find new ways to create, display and retrieve the information that constitutes the Internet.

The following diagram explains how to protect your system while using internet



HOW CAN YOU PROTECT YOURSELF WHILE USING THE INTERNET?

Keep all personal information safe and private

Do not give out your mobile number or address

Always ask permission from others if you are putting their picture online

Learn how to block, delete or ignore people – especially strangers

Respect your friends + family – do not give out their details

Do not trust people you meet online. Online friends are really strangers

Always tell someone if someone makes you feel uncomfortable or worried

Never reply to messages from people you do not know

Fig. 9.2. Protection tips for Using Internet

History & Development of the Internet:

In its infancy, the Internet was originally conceived by the Department of Defence as a way to protect government communications systems in the event of a military strike. The original network, dubbed Arpanet (for the Advanced Research Projects Agency that developed it) evolved into a communications channel among contractors, military personnel, and university researchers who were contributing to ARPA projects. The network employed a set of standard protocols to create an effective way for these people to communicate and share data with each other. Arpanet's popularity continued to spread among researchers, and in the 1980's the National Science Foundation, whose NSFNet, linked several high speed computers, took charge of the what had come to be known as the Internet. By the late 1980s, thousands of cooperating networks were participating in the Internet. In 1991, the US High Performance Computing Act established the NREN (National Research & Education Network). NREN's goal was to develop and maintain high-speed networks for research and education, and to investigate commercial uses for the Internet.

The rest, as they say, is history in the making. The Internet has been improved through the developments of such services as Gopher and the World Wide Web. Even though the Internet is predominantly thought of as a research oriented network, it continues to grow as an informational, creative, and commercial resource every day and all over the world.

The concept of "Internet" has evolved out of a program called APRANET which was developed in order to carry out defence-related research and maintain communication in case computer networks were damaged during war. The Internet has experienced tremendous growth. The importance of internet needs no emphasis. Most people obtain the bulk of their information on matters of contemporary interest from this medium. It plays a great role in shaping the society. It is a powerful instrument, which can be used for greater good as also for doing immense harm to the society. It depends upon how it is used. Although the phenomenon of internet is not as pervasive as the television or radio, as it requires many affirmative steps to be taken before gaining access, but its diversity cannot be undermined. It is as the human thought.

Since the jurisprudence of pornography and obscenity on the internet is developed mostly in the western countries. It becomes necessary to understand the judicial principles evolved by the Courts in those countries, which although do not bind the Indian judiciary but has surely helped in shaping the law in India and may provide necessary guidance to decide cases in the future.

9.2 Civil Remedies in the Case of Obscenity:

The civil remedies in the case of obscenity can be invoked generally in case of defamation. The Code of Civil Procedure, 1908 governs the law relating the jurisdiction of the Civil Courts. It provides that in case of suits filed for compensation for wrong done, which is generally invoked in case of defamation, the suit can be filed either where the act was done or where the defendants resides or personally works for gain. And in all other cases suit can be instituted either where defendant resides or personally works for gain or where cause of action arises either wholly or in part.

9.3 Data Theft and Theft of Internet Hours:

Section 43(b) of the Indian Technology Act 2000, defines Data Theft as

i. Downloading data/information stored in a computer through internet (without the permission of the owner or any other person who is in charge of a computer, computer system or computer network

ii. Downloading copies or extracts any data, computer database or information from such computer network computer system.

The section makes the person liable to pay damages by way of compensation, not exceeding Rs. 1 crore to the person so affected.

Section 378, IPC defines theft as "whoever intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft'.

As far as this definition is concerned it can well include every type of theft with the help of computer, as computer data/information is moveable property and downloading of data can well be said as moving the property in the context of Section 378.

Theft of Internet hours refers to using someone else's internet hours.

9.4 Denial of Access/Denial of Service:

A denial of service (DoS) attack occurs when a malicious user attempts to flood a networked computer or device with traffic in order to make the computer or device unavailable. The attack gets its name from its purpose it is intended to deny the ability of an institution or company to provide service to its users, affiliates or customers.

On the Internet, typical targets of DoS attacks include corporate Websites and e-mail servers, along with IRC and other chat servers and hosts. Within the FAS Network, Harvard's main router providing Internet service and our UNIX login servers/e-mail systems are typical targets. This is one of the most common reasons why Harvard's connection to the Internet and externl sites are lost.

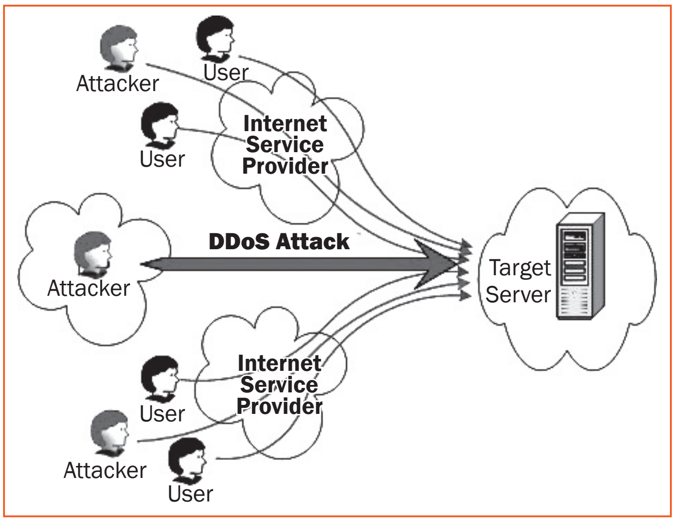


Fig. 9.3. DDoS Attack

In many cases where a DoS attack affects the FAS Network and systems, the attack originates from a student, faculty or staff computer on the network, or from a compromised FAS UNIX account. Typically this happens when a malicious user hacks into the user's system and installs software there to launch a DoS attack.

The legitimate user is prevented from using the service of the computer to which he is legally entitled. Networks are flooded with someone else information and prevent legitimate user from network. It can disable an organization, or any personal computer. Section 43(f) of the information technology Act 2000, provides penalty for culprits who deny the access to the real user.

9.5 General Law of Obscenity in India:

This paper looks into the need to reform outdated laws relating to obscenity in India. Laws which have been abused in order to restrict freedom of expression. The law covering obscenity is dealt with in the India Penal Code of 1860. Interestingly, these laws are relics of the colonial period and fundamentally at variance with the constitutional guarantees of freedom of expression. These laws relating to obscenity are directly inherited from British colonialism. A time where Britain experienced a period of what might be described as 'moral fundamentalist'.

A brief study is done looking into the present obscenity law of India, the history of that law and the surrounding circumstances in which that law came into our statute book and the inadequacy of law. It further looks into the laws dealing with obscenity by different countries.

The general law of obscenity in India can be found in Section 292 of the Indian Penal Code, I860. This section applies to a variety of matters and is comprehensive enough to cover all obscene publications.

It may be mentioned here that by virtue of a State Amendment (Madhya Pradesh Act, 17 of 1999) to Section 320 of Criminal Procedure Code, 1973, "obscenity" which in the context of the amendment would mean either obscene acts or use of obscene words has been made a compoundable offence, at the instance of the person against whom the act is committed.

On 9th June, 2000, the Government of India enacted the Information Technology Act 2000. Although, the preamble would indicate that the focus of the present Act is towards commerce, but the Act contains various penal provisions. The most relevant for the subject under discussion is Section 67.

Thus Section 67 is the first statutory provision dealing with obscenity on the internet. It must be noted that the both under the Indian Penal Code, 1860 and the Information Technology Act 2000, the test to determine obscenity is similar. Therefore, it is necessary to understand the broad parameters of the law laid down by the Court in India, in order to determine "obscenity".

The Indian Penal Code on obscenity grew out of the English Law, which made Court the guardian of public morals. While interpreting the meaning of 'obscenity' the Courts in India have uniformity adopted the test laid down by the English Court in Hicklins Case. The Courts have explained that the Hicklins test does not emphasize merely on stray words, as the words are "matters charged" and to that extent it must be held to *secundum subjectum materiam*, that is to say, applicable to the pamphlet there considered. Thus, the Court must apply itself to consider each work at a time.

There exist a distinction between "obscenity", "pornography" and "vulgarity", while later consists of pictures, writings etc which are intended to arouse sexual feelings whereas the former consists of writing etc which though are not intended to arouse sexual feelings but definitely has that tendency. Vulgarity may arouse a feeling of revulsion, disgust and even boredom but unlike "pornography" or "obscenity" does not have the tendency to corrupt or deprave the minds of a person. However, this concept of obscenity would differ from country to country depending on the contemporary standards of the society.

9.6 Invention of Computers and Increasing Use of the Internet:

With the invention of computers and increasing use - of the Internet and its positive sway on us, has also crept in different types of negative impact and transnational white-collar crimes. Cyber Crime poses a great challenge before the legislature and law enforcement agencies as there may be differences between jurisdictions about whether or not the activity in question has occurred at all, whether it is criminal, who has committed it, who should investigate it and who should adjudicate and punish it. These problems can be solved by legislating laws which are more compatible to fit the requirements to regulate the Cyber Crimes. "There should be given a special training of Investigating Officers,

Frequency of Internet Usage in India

- 3% of People using Internet less than once a month
- 12% of People using Internet 2–3 times in a month
- 18% of People using Internet once in a week
- 19% of People using Internet 4-6 times in a week
- 23% of People using Internet 2-3 in a week
- 25% of People using Internet daily

Police Officials, Judges and Law Enforcing Agents so that they can understand the meticulous and sophisticated nature cyber law and then aid for imparting justice to victims. There should also be a global consensus among nations on what amounts to Cyber Crime and when will the jurisdiction fall for the crime so that the procedures do not delay prosecution of offender which may lead to injustice˝.

9.7 Jurisdiction:

The ability of the Internet to reach across borders has raised a host of questions, including questions of legal jurisdiction. Should defendants be haled to a jurisdiction where, though their websites are accessible, they had no intent to do business? Several recent court decisions on interstate jurisdiction point to the beginnings of a standard for determining whether an entity has "purposefully" directed itself to Internet users in another jurisdiction. At the international level, the disparate legal approaches between countries magnify the potential problems. Without international guidelines on recognizing jurisdiction, exposure to local liability could have a detrimental effect on global business.

As explained above obscenity on the internet has both criminal as well as civil consequences. The remedy that a party takes would necessarily depend on the effect of the act of obscenity. Assuming an offence is committed and the Court is called upon to exercise jurisdiction. Chapter XIII of the Criminal Procedure Code, 1973 governs the law relating to the jurisdiction of Courts with respect to inquiries and trial. It provides that an offence shall ordinarily be inquired into and tried by a Court within whose local jurisdiction it was committed. But where the place of offence uncertain, which means, in case the offence was committed partly in one area and partly in another, or where it is committed in one area but its effect ensues in another, where it has been committed in more than one areas, the offence can be tried by the Court having jurisdiction in any of such area.

In a case where the act becomes an offence because of its ensuing consequences it can be tried either by the Court in whose jurisdiction the act was committed or where the consequences ensued.

It must be noted even the Indian Penal Code applies to an offence committed by an Indian citizen outside the territory of India.

Section 75 of the Information Technology Act 2000 penalizes an offence even if it is committed outside India, by a person of any nationality, irrespective of his nationality.

9.8 Obscenity and Free Expression—Human Rights Features:

A recent newspaper article reported that the government of India "has given up the power to block pornographic websites purely on the ground of obscenity." While the author seemingly lamented this limitation of the government's censorship powers, in fact, the October 2009 amendments to the Information Technology (IT) Act in which the supposed change in the law took place should be subject to scrutiny for the very opposite reason: the amendments actually increase the potential for government intrusion of privacy and liberty.

Although generally reasonable and close in fact to the constitutional standards found in the United States on the subject, a more careful look at the IT Act amendments should provide pause for those concerned about the potential for abuse and arbitrary application of enhanced government powers to limit free speech and expression.

Specially, if in fact, as the article claims, the amendments make it the case that the government can no longer ban websites for obscenity, and only the judiciary can do so in accordance with a prosecution of a case under the Act, then this change is a positive development. Such a change would ensure that some form of due process would be provided to an accused person before a given site is banned.

However, an inspection of the text of the amendments leaves one less convinced than the article's interpretation. According to the relevant Section 69 of the amended Act, an officer of the Central Government can "intercept, monitor, or decrypt" any information from any computer source (including websites) if necessary for the interest "of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence" (emphasis added). In similar fashion, the newly added Section 69-A authorises the Central Government to "block for access by the public" information in any computer resource if necessary for the interest "of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above" (emphasis added). The previous version of the IT Act had a similar definition except that the last portion of the definition stated only "for preventing incitement to the commission of any cognizable offence" without the portion stating "relating to above or for investigation of any offence.

9.9 Protect by the First Amendment to the Constitution:

The primary concern of the Courts in United States of America has been to protect the freedom guaranteed by the First Amendment to the American Constitution. The First Amendment enacts an absolute prohibition on the abridgement of freedom of speech thus imposing a heavy burden on anyone transgressing the right to justify the transgression. Since the constitutional provision contained no exceptions, these had to be evolved by judicial decisions. The Courts have been grappling with the problem of balancing the individual right to speech and expression and the manner of exercising that right. The aim has been to arrive at a decision that would protect the "quality of life" without making "closed mind" a principal feature of an open society or an unwilling recipient of information the arbiter to veto or restrict freedom of speech and expression.

Similarly, in areas of commercial speech it was held that the Government may ban forms of communication more likely to deceive the public than to inform them and commercial speech regarding illegal activity.

It was in the case of Chaplinsky v. New Hampshire, wherein the Courts recognized "obscenity" as an exception to the "free speech" guaranteed under the American Constitution. Although the context of this case was "spoken words", but its significance lay in the recognition of obscenity as an exception to an absolute freedom guaranteed by the American Constitution. However, it was the case of Roth v. United States where the Supreme Court directly dealt with the issue of "obscenity"as an exception to freedom of speech and expression.

This case dealt with the constitutionality of 18 USC 1461 that made punishable the mailing of any material which was "obscene, lascivious, lewd or filthy and other publication of an indecent character". While upholding the constitutional validity of the above Code the Court observed that "obscenity is not within the area of constitutionally protected freedom of speech or press either (1) under the First Amendment as to the Federal Government, or (2) under the Due Process Clause of the Fourteenth Amendment, as to the States." The Court further held that the rejection of "obscenity" was implicit in the First Amendment. Sex and Obscenity were held not to be synonymous with each other. Only those sex-related materials which had the tendency of "exciting laustful' were held to be obscene. According to the Supreme Court, obscenity had to be judged from the point of view of an average person by applying contemporary community standards.

9.10 Protection of Minors:

Internet Safety Tips for Children

- Do not give out personal information such as your address, telephone number, parents' work address or telephone number, or the name and location of your school.
- Tell your parents right away if something that you come across online makes you feel uncomfortable.
- Never agree to see someone you "meet" online without your parents' permission. If they permit a meeting, be sure that it is in a public place and you bring a parent along.
- Never send pictures of yourself or any other personal material to a friend you meet online without telling your parents first.
- Never respond to messages or bulletin board items that are suggestive, obscene, belligerent, threatening or make you feel uncomfortable. Give a copy of such messages to your parents.
- Follow the rules that your parents set for going online and do not access other areas or break these rules without their permission.
- Do not download anything from anyone you don't know.

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program — a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

The moral health of children has always been and would always remain a matter of great concern. The Courts in every jurisdiction are constantly making efforts to protect the minor from the harmful effects of sexually explicit material on the Internet. The Acts of child pornography have been consistently held to be an exception to every constitutional freedom and the Courts and legislator, in order to prevent it from flourishing, have evolved various concepts.

However, it must always be remembered that the goal must always be to strike the right balance between the protection of minor and the interest of the adults. At this juncture, the observations of the Supreme Court of Untied States of America Prince v. Massasnchettes are noteworthy:

Internet Safety Tips for Parents

- Find out what information your computer service provider offers and whether you can block objectionable material.
- Consider using a pseudonym or unlisting your child’s name, if possible. Avoid using online profiles.
- Never allow a child to arrange a meeting with another computer user without permission. Accompany the child to any meeting.
- Do not allow your child to respond to suggestive, obscene, or threatening messages. Forward such messages to your ISP.
- Call the National Centre for Missing & Exploited Children (1-800-843-5678) if you are aware of any online child pornography.
- Never give out personal information about yourself or your child.
- Keep the computer in your family room where you can monitor your child’s activities.
- Share an e-mail account with your child so you can oversee his or her mail.
- Spend as much time as possible online together to show your children proper behaviour and rules.
- Do not allow your children to go into private chat rooms alone.
- Monitor your credit card bill for payments to porn sites.
- Consider using an online service that has special child accounts with restricted access to chat rooms and the Internet.

“It is cardinal with us that the custody, care and nurture of the child reside first with the parents, whose primary function and freedom include preparation for obligation the State can neither supply nor hinder.”

Further, there should not be an insistence to have a standard wherein a writer is always to keep in his mind that a child ought not to be brought in contact with sex, as this would require him to write only adolescent and not adults.

Notes :

अध्याय 10

Chapter 10

Mobile Phone, Privacy and Electronic Surveillance

Notes :

10.1 General:

Recent developments in mobile computing have been fast and furious. In this three-part overview of mobile development platforms, we'll be taking a closer look at this history, starting with a broad overview in this part. Part 2 examines the rise of the iPhone and Android platforms and the final part will look at how this has affected some of the other mobile platforms.

The rapid development of positioning technology and wireless networks has meant that a mobile phone has become an extremely versatile and powerful device. A contemporary mobile phone can make video calls, record and share multimedia, send and receive emails, surf the Internet and take advantage of Global Positioning System (GPS) technology to access Location Based Services (LBS). The combination of these technologies into a compact, stylish and portable device has led to a phenomenal and unprecedented number of mobile phone users. To many of these users, the use of a LBS does not constitute a loss of privacy. Typically a user is not aware of what information they are divulging and where this information is stored. It is important to inform users what information they might be sharing so they can make informed decisions on how their location information is used and handled.

Users of mobile phones are divulging increasingly more information about their location and behaviour based on location data created when using their mobile phone; for simple activities such as making a phone call to more advanced requests such as accessing LBS. Location information can be in the form of telecommunications traffic data collected for billing Purposes or precise location data which records the user's position on the Earth's surface. Telecommunications Traffic data is data that is collected to facilitate billing purposes. Traffic data in mobile phones is not a new concept, as traditional fixed line billing requires the same traffic data to be collected. Penders (2004) explain that traffic data are generated to direct the communications. Types of traffic data collected include the calling number, the dialed number and the time the call started and finished. What is not recorded is the communication itself i.e. the voice conversation (Penders, 2004). Traffic data can be considered sensitive information as it can be ascertained who is calling who and at what time. By looking at the data over time and the length of each call, behavioural patterns can be identified and personal information can be inferred about the mobile phone user. For example, a one off phone call during business hours may indicate a professional and business -like relationship between the caller and the receiver. On the other hand, repeated long phone calls late at night might indicate a more personal relationship. This information can be considered private and should be collected only to facilitate the provision of the service. Furthermore, access to this data should be restricted to those who only require it for the purposes of billing.

One form of electronic surveillance developed by law enforcement results in attaching a ´bug´ to a person's telephone line or to a phone booth and recording the person's conversation. Courts have held that when having a telephone conversation, one would not expect an unknown third-party government agent to listen to the conversation. A person has a legitimate expectation of privacy if the person honestly and genuinely believes the location under search to be private and if the reasonable person under the same or similar circumstances would believe the location to be private as well. Therefore, law enforcement has more leeway when intercepting communications in a public place than when the interception occurs in a secluded environment. The courts have given law enforcement the freedom to record conversation during jail visits, provided that the monitoring reasonably relates to prison security.

Two general categories of electronic communication surveillance exist. Wire communications refer to the transfer of the human voice from one point to another via use of a wire, cable, or similar device. When law enforcement ´taps´ a wire, they use some mechanical or electrical device that gives them outside access to the vocal transfer, thus disclosing the contents of the conversation. Electronic communications refer to the transfer of information, data, or sounds from one location to another over a device designed for electronic transmissions. This type of communication includes email or information uploaded from a private computer to the Internet. Using electronic devices to keep surveillance over a person may implicate the investigated individual's Fourth Amendment rights. One form of electronic surveillance is attaching a ´bug´ to a person's telephone line or to a phone booth and recording the phone conversation. Courts have held that this practice constitutes a search under the Fourth Amendment, which protects an individual's privacy rights for situations in which the person has a legitimate expectation of privacy.

The mobile development community is at a tipping point. Mobile users demand more choice, more opportunities to customize their phones, and more functionality. Mobile operators want to provide value-added content to their subscribers in a manageable and lucrative way Mobile developers want the freedom to develop the powerful mobile applications users demand with minimal roadblocks to success. Finally, handset manufacturers want a stable, secure, and affordable platform to power their devices. Up until now single mobile platform has adequately addressed the needs of all the parties.

Enter android, which is a potential game-changer for the mobile development community. An innovative and open platform, Android is well positioned to address the growing needs of the mobile marketplace.

This chapter explains what Android is, how and why it was developed, and where the platform fits in to an established mobile market place. Mobile phones have become an all encompassing electronic and entertainment device that may include email, a video camera, music and games. Unwanted SMS (Short Message Services), text or picture messages can be particularly annoying. Exercise caution when disclosing your mobile phone number and look for options, such as tick boxes, that allow you to “opt-out” for receiving commercial messages.

10.2 A Brief History of Mobile Software Development:

To understand what makes Android so compelling, we must examine how mobile development has evolved and how Android differs from competing platform.

10.3 A "Free Market" for Applications:

Android developers are free to choose any kind of revenue model they want. They can develop freeware, shareware, or trial-ware applications, ad-driven, and paid applications. Android was designed to fundamentally change the rules about what kind of wireless applications could be developed. In the past, developers faced many restrictions that bad little to do with the application functionality or features:

- Store limitations on the number of competing applications of a given type;
- Store limitations on pricing, revenue models, and royalties;
- Operator unwillingness to provide applications for smaller demographics.

With Android, developers can write and successfully publish any kind of application they want. Developers can tailor applications to small demographics, instead of just large-scale money-making ones often insisted upon by mobile operators. Vertical market application can be deployed to specific, targeted users.

Because developers have a variety of application distribution mechanisms to choose from, they can pick the methods that work for them instead of being forced to play by others' rules. Android developers can distribute their applications to users in a variety of ways.

- Google developed the Android Market, a generic Android application store with a revenue-sharing model.
- Handango.com added Android applications to its existing catalogue using their billing models and revenue sharing model.
- Developers can come up with their own delivery and payment mechanisms.

Mobile operators are still free to develop their own application stores and enforce their own rules, but it will no longer be the only opportunity developers have to distribute their applications.

Android might be the next generation in mobile platforms, but the technology is still in its early stages. Early Android developers have had to deal with the typical roadblocks associated with a new platform, frequently revised SDKs, lack of good documentation, and market uncertainties. There are only a handful of Android handsets to consumers at this time.

On the other hand, developers diving into Android development now benefit from the first-to-market competitive advantages we've seen on other platforms such as BREW and Symbian. Early developers who give feedback are more likely to have an impact on the long-term design of the Android platform and what features will come in the next version of the SDK. Finally, the Android forum community is lively and friendly. Incentive programs, such as the Android Developer Challenge, have encouraged many new developers to dig into the platform.

10.4 Android Application Framework:

Android applications are written in the Java programming language. The Android SDK tools compile the code—along with any data and resource files—into an Android package, an archive file with an.apk suffix. All the code in a single .apk file is considered to be one application and is the file that Android-powered devices use to install the application.

"Be not afraid of anything. You will do Marvelous work. It is Fearlessness that brings Heaven even in a moment."

The Android application framework provides everything necessary to implement your average application. The Android application lifecycle involves the following key components:

- Activities are functions the application performs;
- Groups of views define the application's layout;
- Intents inform the system about an application's plans;
- Services allow for background processing without user interaction;
- Notifications alert the user when something interesting happens.

Android applications can interact with the operating system and underlying hardware using a collection of managers. Each manager is responsible for keeping the state of some underlying system service. For example, there is a location manager that facilitates interaction with the location-based services available on the handset. The View Manager and Window Manager manage user interface fundamentals.

Applications can interact with one another by using or acting as a Content Provider. Built in application such as the Contact manager the content providers, allowing third-party applications to access contact data and use it in an infinite number of ways. The sky is the limit.

10.5 Android Application Runtime Environment:

Android's unique application component architecture is, in part, a product of the way Android implements a multiprocessing environment. In order to make that environment suitable for multiple applications from multiple vendors with a minimal requirement to trust each vendor, Android executes multiple instances of the Dalvik VM, one for each task. In Component Lifecycles, and in later chapters, we will explore how component life cycles enable Android to enhance the way garbage collection works within application heaps, and how it enables a memory recovery strategy across multiple heaps.

Each Android application runs in a separate process, with its own instance of the Dalvik virtual machine (VM). Based on the Java VM, the Dalvik design has been optimized for mobile devices. The Dalvik VM has a small memory footprint and multiple instances of the Dalvik VM can run concurrently on the handset.

10.6 Applications as Operating System Users:

Operating systems provide a software platform on top of which other programs called application programs, can run. The application programs must be written to run on top of a particular operating system. Your choice of operating system, therefore, determines to a great extent the applications you can run. For PCs, the most popular operating systems are DOS, OS/2, and Windows, but others are available, such as Linux.

When an application is installed, the operating system creates a new user profile associated with the application. Each application runs as a different user, with its own private files on the file system, a user ID, and a secure operating environment.

The application executes in its own process with its own instance of the Dalvik VM and under its own user ID on the operating system.

10.7 Application Signing for Trust Relationships:

In a trust relationship, you must provide the SAML-enabled systems with the URLs they need to contact each other. In some transactions, only the system that initiates the transaction (the Secure Access Service) needs to know the URL of the other system. (The Secure Access Service uses the URL to initiate the transaction.) In other transactions (SSO transactions using artifact profiles), you need to configure each system with the URL of the other.

An Android application packages are signed with a certificate, so users know that the application is authentic. The private key for the certificate is held by the developer. This helps to establish a trust relationship between the developer and the user. It also allows the developer to control which applications can grant access to one another on the system. No certificate authority is necessary; self-signed certificates are acceptable.

10.8 Commonly Used Packages:

With Android mobile developers no longer have to reinvest the wheel. Instead, developers use familiar class libraries exposed through Android's Java packages to perform common task such as graphics, database access, network access, secure communications, and utilities (such as XML parsing).

The Android packages include support for

- Common user interface widgets (Buttons, Spin Controls, Text Input);
- User interface layout;
- Secure networking and Web browsing features (SSL, WebKit);
- Structured storage and relational databases (SQLite);
- Powerful 2D and 3D graphics (SGL and OpenGL ES 1.0);
- Audio and visual media formats (MPEG4, MP3, and Still Images);
- Access to optional hardware such as Location-Based Services (LBS), Wi-Fi, and Bluetooth.

10.9 Content Providers—Developing Android Applications:

To develop apps for Android devices, you use a set of tools that are included in the Android SDK. Once you've downloaded and installed the SDK, you can access these tools right from your Eclipse IDE, through the ADT plug-in, or from the command line. Developing with Eclipse is the preferred method because it can directly invoke the tools that you need while developing applications.

When users have Android handsets, they need those killer apps, right?

Google has led the pack, developing Android applications, many of which, like the email client and Web browser, are core features of the platform, OH A members, such as eBay, are also working on Android application integration with their online auctions.

The first Android Developer Challenge received 1,788 submissions—all newly developed Android games, productivity helpers, and a slew of Location Based Services (LBS). We also saw humanitarian, social networking, and mash — up apps. Many of these applications have debuted with users through the Android Marker—Google's software distribution mechanism for Android.

10.10 Developing Android Applications:

The Android SDK provides an extensive set of application programming interfaces (APIs) that is both modem and robust Android handset core system services are exposed and accessible to all applications. When granted the appropriate permissions, Android applications can share data among one another and access shared resources on the system securely.

10.11 Enabling Development of Powerful Applications:

In the past, handset manufacturers often established special relationships with trusted third-party software developers (OEM/ODM relationships). This elite group of software developers wrote native applications, such as massaging and Web browsers, which shipped on the handset as part of the phone's core feature set. To design these applications, the manufacturer would grant the developer privileged inside access and knowledge of a handset's internal software framework and firmware.

On the Android platform, there is no distinction between native and third-party applications, enabling healthy competition among application developers. All Android applications use the same libraries. Android applications have unprecedented access to the underlying hardware, allowing developers to write much more powerful applications. Applications can be extended or replaced altogether. For example, Android developers are now free to design email clients tailored to specific email servers such as Microsoft Exchange or Lotus Notes.

10.12 Explicitly Defined Application Permission:

To access shared resources on the system, Android applications register for the specific privileges they require. Some of these privileges enable the application to use phone functionality to make calls, access the network, and control the camera and other hardware sensors. Applications also require permission to access shared data containing private and personal information such as user preferences, user's location, and contact information.

Applications might also enforce their own permissions by declaring them for other applications to use. The application can declare any number of different permission types, such as read – only or read – write permissions, for finer control over the application.

10.13 Familiar and Inexpensive Development Tools:

Unlike some proprietary platforms that require developer registration fees, vetting, and expensive compilers, there are no upfront costs to developing Android applications.

10.14 Familiar Language, Familiar Development Environments:

Developers have several choices when it comes to integrated development environments (IDE). Many developers choose the popular and freely available Eclipse IDE to design and develop Android applications. Eclipse is the most popular IDE for Android development and there is an Android plug in available for facilitating android development. Android applications can be developed on the following operating systems:

- Windows XP or Vista
- Mac OS X 10.4.8 or later (x86 only)
- Linux (tested on Linux Ubuntu 6.06 LTS, Dapper Drake).

10.15 Forming of the Open Handset Alliance:

With its user-centric, democratic design philosophies, Google has led a movement to turn the existing closely guarded wireless market into one where phone users can move between carriers easily and have unfettered access to applications and services. With its vast resources, Google has taken a broad approach, examining the wireless infrastructure from the FCC wireless spectrum policies to the handset manufacturers' requirements, application developer needs, and mobile operator desires.

Next, Google joined with other like-minded members in the wireless community and posed the following question. What would it take to build a better mobile phone?

The Open Handset Alliance (OHA) was formed in November 2007 to answer that very question. The OHA is a business alliance comprised of many of the largest and most successful mobile companies on the planet. Its members include chip makers, handset manufacturers, software developers, and service providers. The entire mobile supply chain is well represented.

10.16 Free and Open Source:

The Free and Open Source Software (FOSS) model provides interesting tools and processes with which women and men can create, exchange, share and exploit software and knowledge efficiently and effectively. FOSS can play an important role as a practical instrument for development as its free and open aspirations make it a natural component of development efforts in the context of the Millennium Development Goals (MDGs). Android is an open source platform. Neither developers nor handset manufacturers pay royalties or license fees to develop the platform.

The underlying operating system of Android is licensed under GNU General Public License Version 2 (GPL v.2), a strong "copy left" license where any third-party improvements must continue to fall under the open source licensing agreement terms. The Android framework is distributed under the Apache Software License (ASL/Apache2), which allows for the distribution of both open and closed source derivations of the source code. Commercial developers (handset manufacturers especially), can choose to enhance the platform without having to provide their improvements to the open source community. Instead, developers can profit from enhancements such as handset- specific improvements and redistribute their work under whatever licensing they want.

Android application developers have the ability to distribute their applications under whatever licensing scheme they prefer. Developers can write open source freeware or traditional licensed applications for profit and everything in between.

10.17 Freely Available Software Development Kit:

The Android SDK and tools are freely available. Developers can download the Android SDR from the Android website after agreeing to the terms of the Android Software Development Kit License Agreement.

10.18 Google Goes Wireless:

A coalition led by the Web search giant is scoring early wins in a tussle over $10 billion in wireless airwaves. For a company that's had an office in Washington, D.C., for less than two years, Google is wielding a surprising amount of power in the nation's capital.

The Company's initial forays into mobile were beset with all the problems you would expect. The freedom Internet users enjoyed were not shared by mobile phone subscribers. Internet users can choose from the wide variety of computer brands, operating systems, Internet service providers, and Web browser applications.

Nearly all Google services are free and ad driven. Many applications in the Google Labs suits would directly compete with the applications available on mobile phones. The applications range from simple calendars and calculators to navigation with Google Maps and the latest tailored news from News Alerts — not to mention corporate acquisitions like Blogger and You Tube.

When this approach didn't yield the intended results, Google decided to a different approach — to revamp the entire system upon which wireless application development was based, hoping to provide a more open environment for users and developers: the Internet model. The Internet model allows users to choose between freeware, shareware, and paid software. This enables free market competition among services.

10.19 Have you Consented to Receive a Message?

You can consent to receive messages either expressly, or by inferred consent.

Express consent can be given in a variety of ways for example, by filling in a form, ticking a box on a website, over the phone or face-to-face. Sometimes, by completing a competition entry, you may provide your consent to receiving commercial electronic messages from related parties. In addition, it must be made clear to you that you will receive commercial messages from this person or organization in the future. No one can send an electronic message to seek your consent as this is considered a commercial message itself.

Message senders can also infer consent. This can be because you have an existing business or other relationship with the sender.

Some examples of where consent may be inferred are:

- You are a member of a club.
- You are a subscriber to a service.
- You are a client who deals with the sender on an ongoing basis.

Consent may also be inferred if you conspicuously publish your work-related mobile phone number or email address (for example, on a website, brochure, or in a magazine).

10.20 Limited Ad-Hoc Permissions:

Application that act as content providers might want to provide some on-the-fly permissions to other applications for specific information they want to share openly. This is done using ad-hoc granting and revoking of access to specific resources using Uniform Resource Identifiers (URIs).

URIs index contains specific data assets on the system, such as images and text. Here is an example of a URI that provides the phone numbers of all contacts: content: contacts/phones

To understand how this permission process works, let's look at an example.

"One individual may die for an idea; but that idea will, after his death, incarnate itself in a thousand lives. That is how the wheel of evolution moves on and the ideas and dreams of one nation are bequeathed to the next."
- Netaji Subhash Chandra Bosh

Let’s say we’ve got an application that keeps track of the user’s public and private birthday wish lists. If this application wanted to share its data with other applications, it could grant URI permissions for the public wish list, allowing another application permission to access this list without explicitly having to ask for it.

10.21 Making a Complaint about a Message:

Complaints can be made to ACMA about unsolicited commercial electronic messages. Many complaints are about:

- a sender who has not clearly identified themselves;
- a sender who has sent the message without the recipient’s consent;
- a message that has no clear unsubscribe function;
- the recipient has unsubscribed from the service but is still receiving messages.

You can make an enquiry or complaint by completing the online form at www.spam.acma.gov.au. The online complaint form outlines the information that ACMA requires from you, and provides an option for you to indicate if you would be willing to assist ACMA in any enforcement actions that may be initiated against the spammer.

10.22 Manufacturers—Designing the Android Handsets:

Android is an attractive platform for developers, but not all designers share our enthusiasm. Making an app look and feel great across hundreds of devices with different combinations of screen size, pixel density and aspect ratio is no mean feat. Android’s diversity provides plenty of challenges, but creating apps that run on an entire ecosystem of devices is rewarding too.

More than half the members of the OHA are handset manufacturers, such as Samsung, Motorola, HTC, and LG, and semiconductor companies, such as Intel, Texas Instruments, NVIDIA, and Quadcomm. These companies are helping design the first generation of Android handsets.

The first shipping android handset the T-Mobile G1 was developed by handset manufacturer HTC with service provided by T-Mobile. It was released in October 2008. Many other Android handsets are slated for 2009 and early 2010.

10.23 Mobile Operators—Delivering the Android Experience:

After you have the phones, you have to get them out to the users. Mobile operators from Asia, North America, Europe, and Latin America have joined the OHA, ensuring a market for the Android movement. With almost half a billion subscribers, telephony giant China Mobile is a founding member of the alliance. Order operators have signed on as well.

10.24 No Costly Obstacles to Publication:

Android applications have none of the costly and time-intensive testing and certification program required by other platforms such as BRE and Symbian.

10.25 No Distinctions made between Native and Third-party Applications:

Unlike other mobile development platforms, there is no distinction between native applications and developer-created applications on the Android platform. Provided the application is granted appropriate permission, all applications have the same access to core libraries and the underlying hardware interfaces.

Android handsets ship with a set of native applications such as a Web browser and contact manager. Third-party applications might integrate with these core applications and even extend them to provide a rich user experience.

10.26 Premium Services:

To cater to mobile phone owners, many new services for adults and children are now available. A premium service is offered at a price that is higher than a typical telephone call and can provide:

- financial data, horoscopes, weather information and ringtones;
- mobile chat services;
- adult pictures and videos.

10.27 Privacy Technology, and Surveillance:

The information Commissioner, who is responsible for the enforcement of the United Kingdom's data protection and freedom of information legislation, warned in 2004 against the dangers of 'sleepwalking into a surveillance society'. Introducing the report, A Surveillance Society commissioned by-his Office and published in November 2006, the Information Commissioner went further:

"Today I fear that we are in fact waking up to a surveillance society that is already all around us. Surveillance, activities can be well-intentioned and can bring benefits. They may be necessary or desirable— for example to fight terrorism and serious crime, to improve entitlement and access to public and private services, and to improve health-care. But unseen, uncontrolled or excessive surveillance can foster a climate of suspicion and undermine trust. As ever more information is collected, shared and used, it intrudes into our private space and leads to decisions which directly influence people's lives. Mistakes can also easily be made with serious consequences— false matches and other cases of mistaken identity, inaccurate facts or inferences, suspicions taken as reality, and breaches of security."

Concern at these privacy implications of information technology was expressed by Lord Hoffmann when delivering his judgment in the House of Lords in the case of v. Brown:

"My Lords, one of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual. No longer is it necessary to peep through keyholes or listen under the eaves. Instead, more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera, the telephoto lens, the hidden micro-phone and the telephone bug. No longer is it necessary to open letters, pry into files or conduct elaborate inquiries to discover the intimate details of a person's business or financial affairs, his health, family, leisure interests or dealings with central or local government. Vast amount of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat".

The potential dangers were further considered by Lord Browne-Wilkinson VC in Marcel v. Metropolitan Police Commissioner, Documents belonging to the plaintiff had been seized by the police in the course of a criminal investigation. Civil proceedings were also current in respect of the same incidents, and a subpoena was served on behalf of one of the parties to this litigation seeking disclosure of some of these documents. Holding that the subpoena should be set aside, the judge expressed concern that:

"If the information obtained by the police, the Inland Revenue, the social security offices, the health service and other agencies were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state."

As indicated in the above passage, an appropriate balance between privacy—classically expressed in terms of the right to be left alone—and surveillance—representing the wish to discover information about another, is difficult to define. Although initially appearing as opposites, privacy and surveillance are linked almost as if they were conjoined twins.

A wide range of surveys of public opinion evidence strong support for the protection of privacy. Although many of these derive from the United States, in the United Kingdom, the Information Commissioner has commissioned annual surveys of public opinion. In the annual report for 2000, the then Commissioner noted:

"Respondents were read a list of issues and asked to say how important they think each is. The proportion who thought that protecting people rights to personal privacy was very important increased but not significantly from 73% to 75%. In terms of people's hierarchy of priorities the issue remains extremely important. Again only Crime Prevention and Improving Standards of Education are thought to be more important issues by the public."

Subsequent surveys have adopted a different formulation, more closely linked to the Information Commissioner's remit, by asking for respondents' views concerning the importance of protecting personal information. The answers, however, have are remained fairly constant. It contains the results from the 2006 survey.

10.28 Receiving Messages, Promoting Goods and Services:

Among other things, the Spam Act, 2003 regulates commercial electronic messages sent by email, instant messaging and mobile phone messages, such as SMS and MMS (multimedia message services). It is enforced by the Australian Communications and Media Authority (ACMA).

Messages that are selling or advertising goods or services, an interest in land, business or investment opportunities or directing the recipient to a location where goods and services are sold or advertised, are considered to be a commercial electronic message and are covered by the Spam Act.

Any commercial message sent to you that does not meet the following conditions is breaking Australia's spam laws:

- Consent; it must be sent with your consent.

- Identify; it must contain accurate information about the person or organization who authorised the sending of the message.
- Unsubscribe; it must contain a functional 'unsubscribe' facility to allow you to opt out from receiving future messages from that source. Your request must be honoured within five working days.

10.29 Reasonable Learning Curve for Developers:

Android applications are written in a well-respected programming language, Java.

The Android application framework includes traditional programming constructs, such as threads and processes and specially designed data structures to encapsulate objects commonly used in mobile applications. Developers can rely on familiar class libraries, such as Java.net and java.text. Specially libraries for tasks like graphics and database Embedded Systems (Open GL ES) or SQLaite.

10.30 Security and Permissions:

The integrity of the Android platform is maintained through a variety of security measures.

10.31 Spam—Related Information:

For more span—related information, including frequently asked questions, complaint and enquiry online forms and to download Spam MATTERS software, visit the ACMA website at www.spam.acma.gov.au.

10.32 Taking Advantage of all Android has to Offer:

Android's open platform has been embraced by much of the mobile development community — extending far beyond the members of the OHA.

As Android phones and applications become more readily available, many in the tech community anticipate other mobile operators and handset manufacturers will jump on the chance to sell Android phones to their subscribers, especially given the cost benefits compared to proprietary platforms. Already, North American operators, such as Verizon Wireless and AT&T, have shown an interest in Android, and T-Mobile already provides handsets.

If the open standard of the Android platform results in reduced operator costs in licensing and royalties, we could see a migration to open handsets from proprietary platforms such as BREW. Windows Mobile, and even the Apple iPhone, Android is well suited to fill this demand.

10.33 Technical Aspects of the Privacy of Mobile Phone Users:

This heading contains profound technical knowledge about the mechanism of mobile phone networks, security measures adopted by different mobile phone systems and privacy threats. These are three indispensable topics that must be covered if one must honestly and satisfactorily do a comprehensive study on threats related to mobile phones. As a result, a section has been dedicated to each topic in order to easily deliver the working concepts in an organized and understandable manner.

The first section looks into the ins and outs of mobile phone networks. This discussion begins with the clarification of the wired and wireless components of mobile phone networks; afterwards, the reader is taken deeper into the mobile phone network by showing the two divisions in the network based on connections they make with the communicating units. Analog mobile phone systems are revisited with more practical details and special emphasis is laid on their pros and cons. Digital mobile phone systems are carefully introduced with sufficient technical and conceptual details. By comparing the two systems, the advantages of digital over analog mobile phone systems were brought into the view of the reader. This section ends by creating awareness about the flaws in the contemporary mobile phone systems.

The second section focuses on the security measures in the two dominant digital mobile phone systems, global system for mobile communications (GSM) and universal mobile telecommunications system (UMTS). This discussion starts by pointing to the threats posed by opting for communication via a wireless medium, afterwards, detailed conceptual and technical details were provided on the security measures in GSM. This quickly follows by clear delineation of the limitations existing in GSM security by citing cases to validate the claims. Subsequently, UMTS was introduced by pinpointing its features, capabilities and security functions. This section ends with the exposition of the security flaws existing in UMTS and an optimistic remark about the future of mobile communications.

This discussion commences with the technical details of signal interception with reference to pertinent technologies like femtocells and IMSI-Catcher afterwards, the mechanism of man-in-the-middle attack is treated with special emphasis on its key role as the core technique for signal interception. Subsequently, the details of data acquisition from a mobile phone in the framework of forensic analysis are discussed as it covers access to user information via mobile phones. This is quickly followed by the various methods by which a malicious attacker might get access to user information via their mobile phones or through the mobile operators database servers. This section is concluded by a call for practical and reliable security solutions for the contemporary mobile devices.

10.33.1 How Mobile Phone Networks Work:

Mobile phone systems are hybrid of wireless and wired communication systems. This is because the connection between the mobile phone and the serving unit, otherwise known as base station is by wireless communication whereas connection between base stations to a sophisticated switching centre also known as mobile switching centre, is through optical fibers or microwave links. The connection between the base station and the mobile switching centre might be direct or through a controlling unit called base station controller. The role of the mobile switching centre is to connect the mobile phones to other mobile phones or to stationary phones through the public switching telephone network.

In order to expatiate what has been aforementioned about wired communications, it is essential to further expound that the connections between the base stations, base station controllers, mobile switching centre, and public switching telephone network are through optical fiber or microwave links. Knowing these basic functionalities and simple inter relationships between the communication and control units, it can be consequently conceptualized that the connections between the mobile phones and the base stations represent the radio access network, while the connections between the base station and the mobile switching centres and between the mobile switching centres to each other and to the public switching telephone network make up the core network which is also known as the fixed network.

Casting our back into the past, we realize that early mobile phone systems such as the first generation North American system popularly known as advanced mobile phone system (AMPS) used analog signal representation and processing. AMPS is the mobile phone system standard developed by Bell Labs, and officially introduced, after the approval of the Federal Communications Commission (FCC), in the Americas in 1983 and Australia in 1987. During the 1980s and into the 2000s, it was the technology that was in vogue in North America and other localities. AMPS uses a range of frequencies between 824 megahertz (MHz) and 894 MHz. In order to stir competition and control prices, the US government required the presence of two carriers in every market, known as A and B carriers. These carriers are each allocated with 832 frequencies: 790 for voice and 42 for data. A pair of frequencies, one for the transmission and the other for reception of data, is used to create one channel. The frequencies used in analog voice channels are typically 30 KHz wide. This 34 KHz was chosen as the standard size because it gives a voice quality that is comparatively as good as a wired telephone.

Relative to the contemporary digital technology, one will incontrover-tibly observe that AMPS is suffering from many weaknesses since it is an analog technology. An evident flaw is in its inherently inefficient use of the frequency spectrum and the most perturbing of all its shortcomings lies in the fact that it could be intercepted easily using radio receivers called frequency scanners. This claim is best reinforced with an historical account to foster clarity and better understanding. In the 1990s, “cloning” was a technological epidemic that cost the industry millions of dollars. An eavesdropper with expert gadgets can intercept a phone’s ESN (Electronic Serial Number) and MIN (Mobile Identification Number, also known as the telephone number). If an ESN/MIN Pair is intercepted, it could be cloned onto a different phone and used in other areas for making calls without paying such distracting imperfections led to the development and shift to better and more reliable technologies.

Second generation system moved to the digital era but with only voice communication and some sort of data communications. Advances in mobile technology led to the proliferation of third generation systems with added features like multimedia communication, mobile commerce, etc Global system for mobile communication (GSM), code division multiple access (CDMA) and third generation (3G) systems are some of the widely-used digital systems of our time. CDMA refers to a technology designed by Qualcomm in the US, which employs spread spectrum communications for the radio link. Rather than sharing a channel as many other network interfaces do, CDMA spreads the digitized data over the entire bandwidth available, distinguishing multiple calls through a unique sequence code assigned. Successive versions of the IS-95 Standard define CDMA conventions in the US, which is the reason why the term CDMA is often used to refer to IS-95 compliant cellular networks. IS-95 CDMA systems are sometimes referred to as CDMA One. The next evolutionary step for CDMA to 3G services is CDMA2000, TIA/ELA/IS-2000 Series, Release A, based on the ITU IMT-2000 standard.

GMS is a cellular system used worldwide and it was designed in Europe, primarily by Ericsson and Nokia. GSM uses a time division multiple access (TDMA) air interface. TDMA refers to a digital link technology whereby multiple phones share a single carrier, radio frequency channel by taking turns. A packet switching enhancement to GSM wireless networks called General Packet Radio Service (GPRS) was standardized to improve the transmission of data.

The next generation of GSM, commonly referred to as the third generation or 3G, is known as Universal Mobile Telecommunications System (UMTS) and involves enhancing GSM networks with a Wideband CDMA (W-CDMA) air interface.

One of the plenteous advantages of the digital mobile phone systems is the ability to encrypt signals for better privacy and security. Although mobile phone signal is encrypted when it is transmitted over the radio access network, this does not absolutely guarantee the signal privacy because encryption algorithms are not crack-proof and they are susceptible to strategic interception attacks as in the case of the GSM encryption algorithm. Another enlightening and cogent point is about multi-mode phones that can switch from digital mode to analog mode depending on the availability of system coverage. In this scenario, the wireless signal can be transmitted over the radio access network without encryption, while the user, in most cases, is unaware of this threat to his/her privacy.

In conclusion, it should be noted that the two concluding paragraphs, which is in fact a microcosm of this report, made some insightful remarks about the pros and cons of the existing mobile technology. The ultimate goal of these incisive statements is to broaden our horizon, widen our perspective and most importantly, serve as a catalyst towards the amelioration of the existent mobile technology.

10.33.2 Security Measures in Different Mobile Phone Systems:

Data security should be an important area of concern for every small-business owner. When you consider all the important data you store virtually — from financial records, to customers' private information — it's not hard to see why one breach could seriously damage your business.

In order to successfully carry out an in-depth, punctilious and competent investigation into the security measures indifferent mobile phone systems, the scope of this analysis will be limited to GSM and UMTS security as they are in arguably the dominant systems due to their widespread use and universal popularity. Security limitations in mobile communication stem from the fact that communication is wireless, which implies that the transmission and reception of messages is conveyed through the air. This inadvertently creates vulnerabilities that jeopardize the mobile network as eavesdroppers and hackers can exploit these inherent weaknesses and gain free rein over the mobile phone system. With the goal of overcoming some of these shortcomings, security measures were integrated into GSM with the objectives of controlling access to the mobile services and protecting any vital information from being disclosed on the radio path in order to safeguard mobile phone users' privacy. Succeeding paragraphs will be dedicated to the elucidation of these security measures.

The first security measure is anonymity. The goal is to make it difficult to identify the user of the system. Anonymity is provided by the use of temporary identifiers. When a new GSM subscriber switches on his/her mobile device for the first time, the real identity which is also known as the International Mobile User/Subscriber Identity (IMUI/IMSI) is used and a Temporary Mobile User/Subscriber Identity (TMUI/TMSI) is then issued to this subscriber. From then on, the temporary identifier is used. The only possible means of determining the temporary identity being used is by tracking the user. Consequently, the use of TMUI, prevents the recognition of a GSM user by a potential eavesdropper or hacker.

In addition to anonymity, another security measure is authentication. The reason for the inclusion of this security feature is for the operator to know who is using the system for billing purposes. This security function checks the identity of the holder of the smart card and then decides whether this mobile device is allowed on a particular network. The authentication by the network is done by a challenge-response mechanism. A random 128-bit number (RAND) which is also known as authentication challenge is generated by the network and sent to the mobile device. The mobile device uses this RAND as an input and through A3 algorithm using a secret key K, (128 bits) assigned to that mobile device, encrypts the RAND and sends the signed response (SRES-32 bits) back. Network performs the same SRES process and compares its value with the response it has received from the mobile device so as to check whether the mobile device really has the secret key. Authentication becomes successful when the two values of SRES match thus enabling the subscriber to join the network. As a consequence, security is achieved because every time a new random number is generated, eavesdroppers and hackers do not get any relevant information by listening to the channel.

The last security measure is user data and signalling protection. The goal of user data protection is to secure user data passing over the radio path and the objective of signalling protection is to ensure that sensitive information on the signalling channel, such as telephone numbers, is secure over the radio path. To protect both user data and signalling information, GSM utilizes a cipher key. After the authentication of the user, the A8 ciphering key generating algorithm which is stored in the SIM card is used. Taking the RAND and K, as inputs, it results in the ciphering key K. To encipher or decipher the data, this K (54 bits) is used with the A5 ciphering algorithm. It must also be mentioned that A5 is performed by the mobile itself and not the SIM card, since it is a strong algorithm that needs relatively high processing capacity which is hard coded in the hardware of the mobile device for the encryption and decryption of data while roaming.

10.33.3 Privacy Threats from Technical Perspectives:

Vast stores of sensitive details about you are living in computer networks all over the world. This is information — secrets shared in e-mails, details of your finances, records of your purchases and disease diagnoses — that you may consider extremely private. Well, businesses, governments and crooks alike think this information is valuable, too, and want control. We've isolated the top 12 threats to your privacy posed by todays technologies and come up with some tips on what you can do to protect yourself. Click on 'Next' below to take a look.

After covering the essence of the mobile communication technology, it is vital to crown our understanding with a painstakingly careful and accurate account of the technical foundations underlying threats to mobile phone users' privacy. The provisioning of this technical account is the goal of this section. The strategy is to sequentially examine the ins and outs of signal interception, access to text messages, access to user records and access to stored information on mobile devices. These are four dominant threats and they will be subjected to adequate clinical analysis in the succeeding paragraphs.

In order to concretize the technical details pertaining to signal interception, it is better to discuss the tools before the technique. This will foster a quick and easy understanding of concepts

Any man who stands for progress has to criticize, disbelieve and challenge every item of the old faith.
- Shahid Bhaghat Singh

as the investigation cuts deeper into technical complexities. To start with, two surprisingly powerful devices will be examined. They are femtocell and IMSI-Catcher. A femtocell, originally known as an Access Point Base Station, is a small cellular base station, typically designed for use in residential or small business environments. It connects to the service provider's network via broadband such as digital subscriber line (DSL) or cable. A femtocell allows service providers to extend service courage indoors, especially where access would otherwise be limited or unavailable. The femtocell incorporates the functionality of a typical base station but extends it to allow a simpler, self contained deployment. Although much implementation attention is focused on UMTS, this concept is also applicable to all standards, including GSM, CDMA2000, Time Division Synchronous Code Division Multiple Access (TD-SCDMA) and Worldwide Inter-operability for Microwave Access (WiMAX) solutions.

Although femtocell is a technology designed to meet benevolent needs, reports are recently emerging on how to secure this technology from being used for malevolent purposes such as unauthorized access and/or service theft, fraud and ID theft, privacy and confidentiality violations, etc The underlying technique which can be used by malicious attackers is man-in-the-middle attack and unfortunately there are two ways to implement this with femtocells. The first method is to directly intercept the signal that is being conveyed on the DSL link, from the femtocells to the base station and the second way is to deploy decoy femtocells to which mobile phones will be connected to unknowingly. The inevitable consequence of any of these means is signal interception and illegal acquisition of confidential and/or vital information. On the other hand, an IMSI-catcher is congenitally a malicious device. It is specially designed for forcing the transmission of the International Mobile Subscriber Identity (IMSI) and intercepting GSM mobile phone calls. It exploits a well-known security flaw in GSM which is the fact that the GSM specification requires the handset to authenticate to the network, but does not require the network to authenticate to the handset. Consequently, the IMSI-catcher pretends to be a base station and stores the IMSI numbers of all the mobile stations in the area as they attempt to connect to the IMSI-catcher. It induces the mobile phone connected to it to use no call encryption, thereby making the call data easy to intercept and convert to audio. By paying close attention to the method adopted here, one would easily reach the conclusion that it is a variation of man-in-the-middle attack.

From what has been aforementioned in the previous paragraphs, it can be deduced that the underlying technique giving these devices the capability to intercept signals is essentially the man-in-the-middle attack. As a consequence, the focus of the current investigation will shift from the tools to the said technique. The best way to do this is to highlight the pertinent findings of an excellent research paper on a man-in-the-middle attack on UMTS. The researchers claimed that the attack allows an intruder to impersonate a legitimate GSM base station to a UMTS subscriber irrespective of the fact that UMTS authentication and key agreement are used. Resultantly, an eavesdropper can listen to all mobile-station-initiated traffic.

In order to execute this attack, the researchers assumed that the attacker knows the IMSI of his/her victim. This is quite realistic because the attacker can easily obtain the IMSI from the mobile device by initiating an authentication procedure prior to the attack and then disconnecting from the mobile device after receiving the IMSI. Having established this, the attack is divided into two phases which will be lucubrated in the following paragraphs.

In the first phase, the attacker acts on behalf of the victim's mobile phone in order to obtain a valid authentication token from any real network by following the enumerated steps: (1) During the connection setup, the attacker sends the security capabilities of the victim's mobile device to the visited network, (2) the attacker sends the TMSI of the victim's mobile device to the visited network. In the case where the TMSI is unknown to the attacker, he/she sends a false TMSI which unfortunately cannot be resolved by the network, (3) if the network cannot resolve the TMSI, it sends an identity request to the attacker and the attacker will reply with the IMSI of the victim, (4) the visited network requests the authentication information for the victim's mobile device from its home network, (5) the home network provide the authentication information to the visited network, (6) the network sends the authentication challenge and authentication token to the attacker, and (7) the attacker disconnects from the visited network.

In the second phase, the attacker impersonates a valid GSM base station to the victim's mobile device by observing the following steps:

1. the victim's mobile device and the attacker establish a connection and the mobile device sends its security capabilities to the attacker;
2. the victim's mobile device sends its TMSI or IMSI to the attacker;
3. the attacker sends the mobile device the authentication challenge and the authentication token that was obtained from the real network in the first phase of the attack;
4. the victim's mobile device successfully verifies the authentication token;
5. the victim's mobile device replies with the authentication response;
6. the attacker gains control and chooses to use "no encryption" or weak encryption which might be a cracked version of the GSM encryption algorithms; and
7. the attacker sends the mobile device the GSM cipher mode command including the chosen encryption algorithm.

After this phase, the attacker gains free rein over the desired communication network and the ultimate goal, signal interception, is achieved.

From the description of this technique, it is vivid that there are challenges and limitations when it comes to the effectuation of this technique but we must bear in mind that it is not impossible especially with the recent increase in speed and computational power of technology gadgets. On a final note, this attack is in fact due to the inherent flaw in GSM technology which is the provision of only access security and not protection against active attacks. As a consequence, user traffic and signalling information such as cipher keys and authentication tokens are sent in the clear over the network which makes them vulnerable to interception and/or impersonation.

10.34 The Open Handset Alliance:

An organization founded in 2007 by Google, T-Mobile, QUALCOMM, Motorola and others that sponsors and promotes the Android open mobile phone platform. Based on Linux, Android was developed to compete with all cell phone platforms including Windows Mobile and Apple's iPhone by offering an open platform that encourages third-party application development. For more information, visit www.openhandsetalliance.com. Enter, search for advertising grant Google. Now a household name, Google has shown an interest n spreading its brand and suite of tools to the wireless marketplace. The company's business model has been amazingly successful on the Internet, and technically speaking, wireless isn't that different.

10.35 Threats and Risks to the Privacy of Mobile Phone Users:

This heading is a comprehensive yet interesting treatise on the existent and imminent threats facing the mobile phone users. These threats can be broadly categorized into two, namely; signal interception and access to user information. Access to user information can be subdivided into access to text messages, access to user records and access to stored information on mobile phone sets. These four threats are the germs upon which the first four sections of this heading were developed.

The first section commences by highlighting the background concepts underlying signal interception. This is followed with a proper definition for signal interception with special emphasis on the possible regions in the mobile phone network where signals can be intercepted. Afterwards, the reader is made to be aware of the some hardware and software techniques that can accomplish the task of signal interception. Upon discussing this, a critical review of analog mobile phone system is done and at the same time, analysis of the contemporary digital mobile phone system is done to reveal its vulnerabilities. This section ends with the discussion of pertinent cases to substantiate the claims made earlier in this section.

The second section begins with a systematic introduction of text massaging to the meaning of access to text messages. Afterwards, this section points to the fact that law enforcement agents have access to text messages. After discussing this point, instances were cited to buttress this claim. Subsequently, the threats from malicious attackers were also brought into view with cases to validate the existence of such threats. This section ends with the mention of the combination of software and/or hardware tools for data recovery.

The third section starts with a coherent description of what user records are and where they can be found. This is followed with the discussion of the various ways by which user records can be accessed from the mobile phone or the operator's database server. This section ends with citing of relevant cases to reinforce the explanations made earlier in this section. The fourth section commences the description of modern mobile phones and how they competently perform the role of data processing, storage and transmission. Subsequently, the different scenarios by which stored information can be accessed is brought to the reader's attention. This section ends with convincing real life instances to support the explications made earlier in this section.

The fifth section is an exploration of other possible threats. The first issue to be looked upon is the possibility of using a mobile phone for tracking and locating a person. This was adequately supported with a news report. The other issue that was investigated in this section is the possibility of malicious threats to mobile phone users as a result of Bluetooth technology. This was also sufficiently reinforced with a news report touching every nook and cranny of the issue. This section is concluded by a call for pragmatic and reliable mobile security solutions.

10.35.1 Signal Interception:

The unifying framework of the spectral-correlation theory of cyclostationary signals is used to present a broad treatment of weak, random signal detection for interception purposes. The relationships among a variety of previously proposed ad hoc detectors, optimum detectors, and newly proposed detectors are established. The spectral-correlation-plane approach to the interception problem is put forth as especially promising for detection, classification, and estimation in particularly difficult environments involving unknown and changing noise levels and interference activity. A fundamental drawback of the popular radiometric methods in such environments is explained.

Before delving into the details of signal interception, it is of utmost importance to trace its root back to its ancestor — eavesdropping. Eavesdropping is simply the act of secretly listening to a private conversation which can be viewed as either unethical or advantageous depending on the parties involved in this act and the underlying motives for indulging in such sact. It can be done over telephone lines (phone tapping), email, instant messaging, and other modes of communication considered private. It must be highlighted at this juncture that signal interception technically falls under phone tapping. Consequently, a brief explanation of what phone tapping is will undoubtedly shed more light on what signal interception really is.

Phone tapping is the monitoring of telephone and internet conversations by covert means with the aim of gaining knowledge about the transmitted information and/or altering this information. Hence, in this context, signal interception can be simply described as the acquisition and/or interruption of data which is being transmitted on the radio access network which represents the connections between the mobile devices and the base stations or on the core network which constitutes the connections between the base station and the mobile switching centres and between the mobile switching centres to each other and to the public switching telephone network.

The issue of signal interception or eavesdropping has evolved in a dramatic manner from an occasional topic of discourse of technological insiders into a daily subject matter of everyone in the mobile communication community due to the undesirable effects that ensue from such hostile attacks. The rampant proliferation of signal interception hardwares. and the realization of software techniques to make mobile devices hackprone are all irrefutable evidences buttressing the fact that signal interception is a major threat to all mobile customers privacy.

10.35.2 Access to Text Message:

It is imperative to provide sufficient explanation of the fundamental concepts underlying the act of accessing text messages before prodding into the access issue. As a consequence, key concepts will be highlighted. Text messaging is the common term for the sending of text messages from mobile phones using services such as. Short Message Service (SMS) on GSM, SkyMail on JPhone, Short Mail on NTT Docomo, SMTP on RIM Blackberry,etc These text messaging services are communications protocol allowing the interchange of short text messages between mobile devices and as mentioned earlier, such services are available on most mobile devices with on-board wireless telecommunications. From the conceptual elucidations provided, access to text messaging can be described as the acquisition of stored or even deleted text messages from users' mobile device or operators' servers by special parties (mobile operators, law enforcement officers or hackers) for legal or illegal purposes.

Law enforcement officers have no problem with obtaining records of text messages and telephone conversations from the mobile operators. In fact, they gain access to such information quickly with ease in their electronic format for meticulous scrutiny. Private detectives working in Poland provide their clients with access to the text message archives of the person under surveillance, especially when investigating someone's private life.

To further substantiate these claims, it will be of vital importance to mention Disk labs Forensics Services that offers thorough mobile phone forensic investigative analysis. Upon request, they provide comprehensive report about the mobile phone user and all data and records contained therein. For instance, with respect to SMS, they provide detailed information about the SIM card, SMS memory usage and confidential details about the SMS message itself like the originating address and the complete text that was sent.

These points to the fact that data stored or transmitted via mobile phones are not fully secure due to the vulnerability of mobile phones.

Researchers at Independent Security Evaluators (ISE) have shown that hackers can take control of an iPhone and gain access to text messages and contact information. Furthermore, they demonstrated that by tricking the phone into accessing a particular website, or by using a rogue Wi-Fi connection, hackers could take complete control of the device and force the phone to send personal information of the mobile user such as text messages and contact numbers.

There are numerous instances where some parties have exploited these inherent flaws in mobile devices and hence infringing on users' personal life.

An interesting case is the text-messaging sex scandal between Detroit's Mayor Kwame Kilpatrick and his chief of staff Christine Beatty. The Detroit Free Press examined over 14,000 text messages obtained from Beatty's pager, publishing those that confirmed the two were having an affair and lied under the oath about it.

To make the cases cited in the previous paragraph more understandable, it will be necessary to explain the technicalities underlying access to text messages. When a mobile phone user sends text messages using his/her mobile phone (for example, SMS messages using GSM), these messages can be intercepted in the same way as voice signals are intercepted. Furthermore, most of the mobile operators keep text messages on their servers for certain duration of time ranging from few days to even years.

As a consequence, when the text messages are available at the operators servers, these messages can be accessed by the mobile operators and/or law enforcement officers. In the light of what has been mentioned, hence it must be put into cognizance that getting access to the stored text messages (by any third party) is a very challenging task but it is possible giving the requisite expertise and tools.

The advent of software that can competently recover and restore deleted text messages which are stored in the SIM card of users' mobile phone and with a more powerful combination of software and hardware that can download entire contents of SIM card signifies a pressing need for reliable security solutions for mobile phones. All that has been meticulously and comprehensively explained points to the essential fact that there is a pressing need for authentic and practical security solutions for threats to mobile users' privacy, especially when it comes to the illegal and unauthorized access to text messages.

10.35.3 Access to User Records:

A concise description of what constitutes user records in a mobile phone will be essential for the proper understanding of the mechanism of how mobile customers' privacy can be breached as a result of unauthorized access to their records on their mobile devices. Mobile customers' records at the mobile network operators' servers are predominantly confidential information. The largest percentage of users' confidential information lies in calling activities such as logs of incoming and outgoing calls; detailed information about dialled and dialling number; precise and detailed records of times and duration of phone calls; user location at times of phone calls; billing information, etc These data are usually managed by the mobile network operator. Just like the case of text message security, having access to the users' record by a third party is a tough and challenging task but it is possible as there are recent cases of infringement of mobile phone users' privacy by accessing their records.

There are also cases where the mishandling and mismanagement of data on storage devices or even hardcopies of such data by the operator can pave way for intrusion and acquisition of information. It must also be noted that the technique for accessing user records is the same with the one mentioned in the previous section about accessing text messages.

The soaring list of mobile phone spy software's website and tutorials caused a great deal of concern to savvy technical insiders, business experts and even government officials to the extent that a senate congress was held for the sole purpose of addressing the issue of protecting consumers phone records. This is to reinforce the claim that access to mobile phone users' record is a major threat to be reckoned with by looking for reliable security solutions that will protect mobile phone users' privacy.

To buttress what has been aforementioned in the previous paragraph, a number of recent and popular cases will be discussed. It is more befitting to commence with an interesting and recent case which in this case is a flashback to the anti-governmental food riots in the Egyptian town of Mahalla el-Kubra. In the midst of the outcry, a large number of protesters carried cell phones which were used to make calls and send text messages. About nine months after this incidence, 22 people were convicted as a result of their involvement in the demonstration. This is utterly enervating especially when one ponders on how the government mysteriously identified and nailed the protesters. Interestingly, this seeming mystery was demystified when Annie Mullins, Vodafone's global head of content standards, declared in a Westminster Forum event that they were forced by the Egyptian authorities to handover customer communications data following the food riots. This is unquestionably a big ethical dilemma related to the retention and release of mobile phone users' records.

10.35.4 Access to Stored Information on Mobile Phone Sets:

A lot of people use their cell phones as portable computers, which ensures they store plenty of sensitive information on their devices. With the rise of the smart phones this trend is accelerating, which can potentially lead to situations where the personal information stored on your phone is compromised.

Due to the numerous advances in Mobile Technology, mobile phones are now equipped with more advanced and better features in addition to the existing standard voice functionality. Consequently, current mobile devices are built to support many additional features and accessories, such as communication protocols for text messaging, email, packet switching for access to the internet, gaming, Bluetooth, infrared, camera with video recorder and (Multimedia Messaging Service) MMS for sending and receiving photos and video, MP3 player, radio and GPS. These whole spectrum of functionalities and the data they process as input or output constitutes the information stored on mobile phone sets.

It must be put into consideration that whenever a mobile device is lost or stolen, all information stored on the mobile device will become available to those who have access to the device even if the stored is password protected. Once again, this emphasizes how vulnerable mobile phones are. A lot of mobile phone users erase the stored information before selling or discarding old mobile phone sets but doing this does not necessarily guarantee security and privacy of the stored information˝ since it is possible, using special software programs, to restore the deleted information." Access to stored information on mobile phone sets by intruders can occur even if the user did not lose/sell his/her mobile phone set. This can be competently done by a skilled intruder through devices like mobile phones, computers and others that are equipped with Bluetooth connection.

In order to adequately substantiate what has been aforementioned in the previous paragraph, some cases will be presented. Adam Gowdiak, a 29-year old Polish security researcher with the Poznan Supercomputing and Networking Centre found two vulnerabilities in the cell phone version of Sun Microsystems' Java Software that under unusual circumstances could let a malicious program read private information from a mobile phone or even render the phone unusable. He figured out how to attack a Nokia 6310i mobile phone but before the vulnerabilities could be exploited, a mobile phone user would have to download and run a malicious Java program. With the rampant usage of web media facilities via the mobile phone by enthusiastic users, this can be a lethal decoy and many users will fall prey to it.

A perturbing case is that of Miley Cyrus whom a unanimous hacker preferred to be known as `K Dollars' camouflaged himself to the operator as being the legitimate owner of her account on the operator's database, consequently, he received her data from the operator by knavishly requesting for it. Her cell phone was also hacked into and some stored pictures was posted and distributed on various websites. Another case is an iPhone embarrassment that makes it simple to access stored information from seemingly locked phones. It was exposed that an unauthorized user can exploit the inherent security flaws in the phone by simply double-pressing the button to make an emergency call. This brings up the user's preferred contacts and clicking on a number provides full access to the phone's features. Furthermore, clicking on an e-mail provides access to all e-mail and clicking on a contact name provides full access to all contacts data. This is another evident proof compelling serious action on mobile phone security due to their apparent gullibility and vulnerability.

10.35.5 Other Threats:

Mobile phones have advanced tremendously beyond our imagination from a mere communication device to intelligent gadgets for upholding justice or in the other sense, smart tools for committing crimes. What can a mobile phone reveal? Surprisingly, much more than we might even want to disclose ourselves. If someone travels with a mobile phone, the device informs network transmitters about the change of that person's location frequently. By analyzing the speed at which radio waves travel, and employing the use of the triangulation technique, it is possible to determine the precise location of a person using his/her mobile phone for text messaging or calls, with a striking accuracy as that of GPS satellite navigation systems.

A news report explored every nook and cranny of mobile phone tracking by stating that mobile telephone technology is fast becoming a powerful tool of investigation in the hands of police investigators. By verifying the Call Data Record (CDR) maintained by cell phone companies, police investigators can access stored data on cell phone location and calls made by subscribers. Police can also reconstruct, down to the minute, the location of a cell phone user at any given time. The standard radio-tracking technology used by cellular companies makes it possible for police to gain valuable information about the precise location of a suspect.

A mobile telephone is usually associated with one particular individual and provides his/ her minute-by-minute location. The technology detects the radio frequency sent from the mobile phone to service antennas. A method called triangulation helps the company detect the caller's whereabouts within its multi-antenna area of operation Surveillance of mobile phone locations is done by measuring the signal strength from the phone to nearby towers. The company can get and store information about any cellular phone that is turned on and operating within the cellular network. This is because cell phones transmit handshaking signals to nearby cell phone towers to let them know that the phone is on and within the range of the cell tower.

10.36 Withdrawing Consent:

A business must make it easy for people to unsubscribe from electronic mailing lists. Unsubscribe instructions must be presented in a clear and conspicuous way must be honoured within five working days and must be at low cost, or no cost, to you (for example, in the case of SMS unsubscribe facilities, a 1800 telephone number would be acceptable).

अध्याय 11

Chapter 11

E-Commerce

Notes :

11.1 Introduction:

Two years ago, the sum total of knowledge about e-commerce could be contained in one bucket of bits. Two years from now, one might float on an ocean of digital signature regulation alone. Almost every area of substantive law has been touched by an e-issue and it is all a cyber - attorney can do to keep his or her head above water. The broadest definition of e-commerce is "the conduct of transactions by electronic means. In the interest of water safety, this series will sail in a smaller pond. We will focus specifically on purchases of goods and services from online stores on the Web. Perhaps the most significant characteristic of the Internet is its fluid and ephemeral character. Web pages disappear in the blink of an electronic eyelash. Users pass through cyberspace at speeds formerly restricted to comic book *Superheroes*. Identity is largely self-selected. Rights are speculative, remedies ethereal. The technology is changing daily, creating a continuous stream of new causes of action. The law comes striding slowly, ponderously through the eddy, leaving footfalls in the mud that are sometimes deep enough to cause diversion in the flow, but are more often irrelevant to the traffic that continues swimming along the surface. Nonetheless, legislative beavers and social engineers have lost their fear of the water and have begun busily constructing their dams and bridges. In unprecedented fashion, they are reaching across the waters to like-minded enthusiasts on the other side, seeking a uniformity of design that will result in stronger spans. One wonders how much longer the stream will flow with full force and abandon.

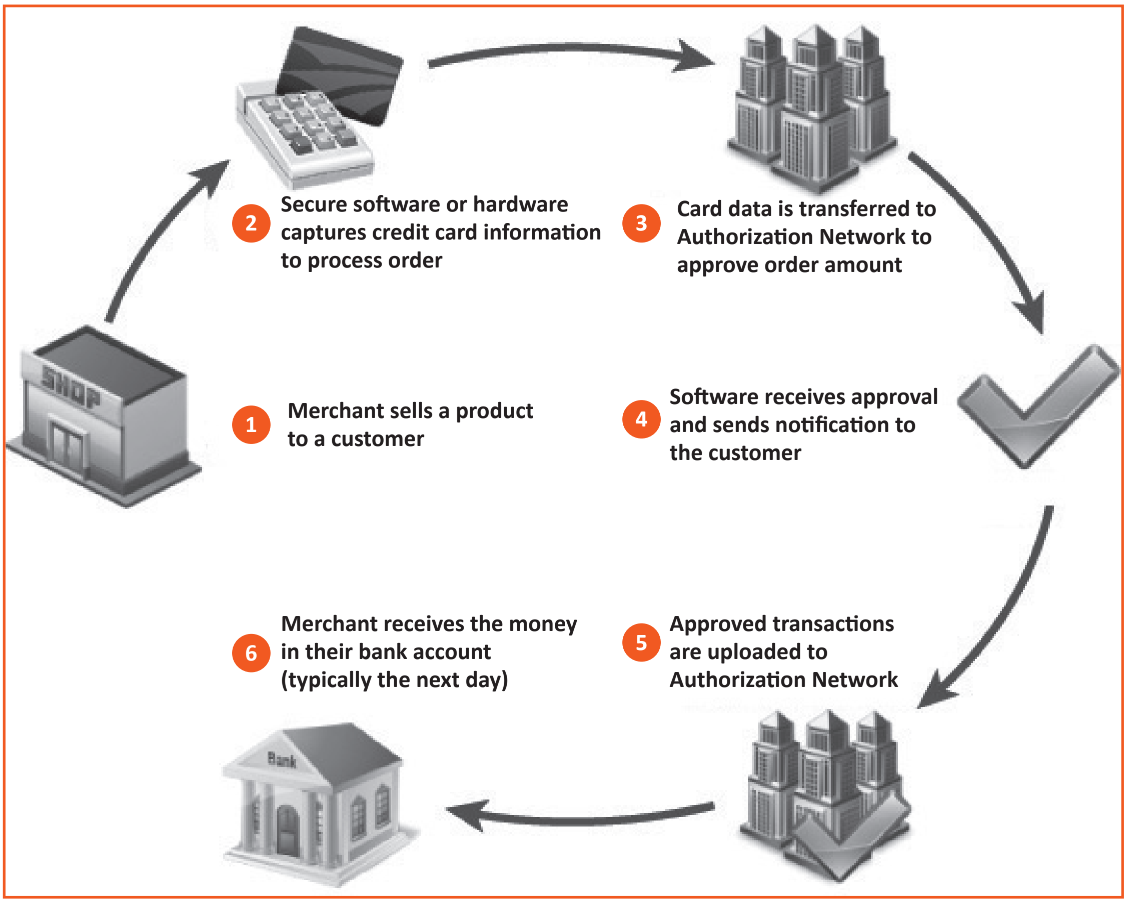

2 Secure software or hardware captures credit card information to process order
3 Card data is transferred to Authorization Network to approve order amount
1 Merchant sells a product to a customer
4 Software receives approval and sends notification to the customer
6 Merchant receives the money in their bank account (typically the next day)
5 Approved transactions are uploaded to Authorization Network
SHOP
Bank

Fig. 11.1. E-Commerce

Different Stages in E-Commerce Process:

This series will look primarily at those steps in the e-commerce venture that are unique to the online experience itself such as the terms of hosting and website development agreements, common advertising arrangements, digital signatures, encryption technology, consumer privacy, and the emerging field of online dispute resolution. It is designed primarily for use by practicing attorneys who are new to e-commerce. Our time is unfortunately too limited to cover many important e-commerce developments. For example, the first thing a start-up might do is set up its corporate structure, establish ownership shares, line up a management team, hunt for seed or paid-in capital, rent an office, and hire staff.

At this stage of Internet development, it is often the case that the information presented today is obsolete by tomorrow. This lecture is only a glimpse of today's e-commerce legal issues. The flow of information continues to change as new issues driven by new technology come to the surface. We hope that this series will help the practitioner steer around some of the larger shoals in the stream of e-commerce.

E-commerce refers to the online selling of products and services through a website for which the payment is usually made online through credit card payments. However, e-commerce transactions may also take place through payment of cash on delivery (COD). e-commerce may involve business-to-business (B2B) or business-to-customer (B2C) transactions. The growth of e-commerce business in India is still at the nascent stage, but is expected to involve many more consumers and grow significantly in the future. Unlike in the US, online purchases in India are still by and large restricted to purchases of airline/train tickets and through online auctions. It is still not common for consumers to do their regular grocery shopping online. However, it is anticipated that middle class consumers will soon begin to purchase an increasing amount of goods and services through the internet as online purchases eliminate the geographical and time constraints of physical purchases.

E-commerce transactions raise many legal issues. The first set of issues is regarding contract formation, that is, at what time is the offeree considered as having accepted the offer and determining the exact time of communication of acceptance of the offer. Additional issues are raised by shrink wrap and click wrap contracts which have evolved due to the nature of the internet where, in order to protect vendors, consumers must undertake contractual obligations before making online purchases.

An online payment through credit cards is a key-element of an e-commerce transaction. Therefore, an understanding of how electronic payment gateways, in particular issues raised under Indian law is central to an analysis of legal issues relating to e-commerce.

E-commerce transactions clearly raise security issues as the customer divulges personal information when making his payments through his credit card. Moreover, neither the cardholder nor the card is physically present in online credit card transactions. All e-commerce transactions are cardholder not present (known as CNP) transactions — the type of transaction in which most credit card fraud occurs in India. Therefore, online payments have to ensure the privacy of information and procedures so as to enable the customer, the merchant and the bank to identify each other and avoid credit card fraud.

In addition to contractual disputes, e-commerce business is particularly prone to giving rise to various other types of disputes. The first type of dispute relates to deceptive trade practices such as false advertising claims and violation of advertising codes and regulations. Online disputes may arise from the commission of offences such as using websites for displaying child pornography or displaying other illegal content in various jurisdictions such the famous French case involving Nazi memorabilia discussed later in this chapter. Therefore, jurisdictional issues, that is, determining which country's courts will have jurisdiction over a dispute involving parties in different countries and arising from a website accessible in every country of the world are critical issues relating to e-commerce.

In addition to determining which country's courts have jurisdiction over the owner of a website which can be accessible internationally, another important legal issue is which country can claim tax revenue generated by the website. International taxation issues arise from e-commerce transactions which are inherently cross-border.

This chapter examines the following legal issues relating to e-commerce:

1) Formation of E-Contracts and Key Contractual Issues
2) Electronic Payment Gateways
3) Security Issues
4) Taxation
5) Foreign Investment in E-commerce Business.

11.1.1 Formation of E-Contracts and Key Contractual Issues:

An electronic contract or an e-commerce agreement encompasses all kinds of commercial contracts that are concluded over an electronic medium or network, that is, the internet. In e-commerce, the exchange of draft contracts in paper form is replaced by instantaneous electronic communications through emails and the internet.

The Indian Contract Act, 1872 governs the formation of all contracts in India. Section 10-A of the IT Act 2000, as amended by the Information Technology (Amendment) Act, 2008 validates contracts concluded in electronic form as legally binding. Section 10-A of the IT Act, as amended, states that

S. 10 - A. Validity of Contracts Formed through Electronic Means:

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in the electronic form or by means of electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

11.1.2 E-Payments/Electronic Payment Gateways:

The Government e-Payment Gateway (GePG) is envisaged to provide a payment gateway for the Civil Ministries and departments with the specific objective of leveraging the existing IT capabilities of the Core Banking Systems and application software functionalities of the CGA's organization towards the development of an integrated payment and accounting system for all levels of usage with seamless interface and data communication. This would result in the elimination of physical cheque processing system and traditional issues associated with it, which would ensure major cost savings for the department by greatly enhancing the overall payment processing efficiency; Online reverse file (payment scroll) giving MIS on unique e-Authorization ID for all e-payment fund transfers; Online auto-reconciliation to facilitate major savings in time and efforts and speed up the compilation of accounting processes; and Ensuring a secure single point data capture of transaction data thereby eliminating duplication of work and data inconsistency.

The online payment process involves credit card payments or electronic fund transfers. In order to make credit card payments for online payments, an electronic payment gateway is required. A payment gateway is an e-commerce application service provider which authenticates an online buyer and seller, enables real-time credit card processing online and protects credit card information given over the internet by connecting the merchant with the financial institutions through which the payment is made. Payment gateways connect the customer making the payments and the merchant by encrypting sensitive information so as to ensure that the credit card details are passed only from the customer to the merchant and the payment processor in a secured manner. In addition, a credit card interchange provides information regarding the availability of funds in the credit card account of the customer and communicates the information to the merchant bank processor.

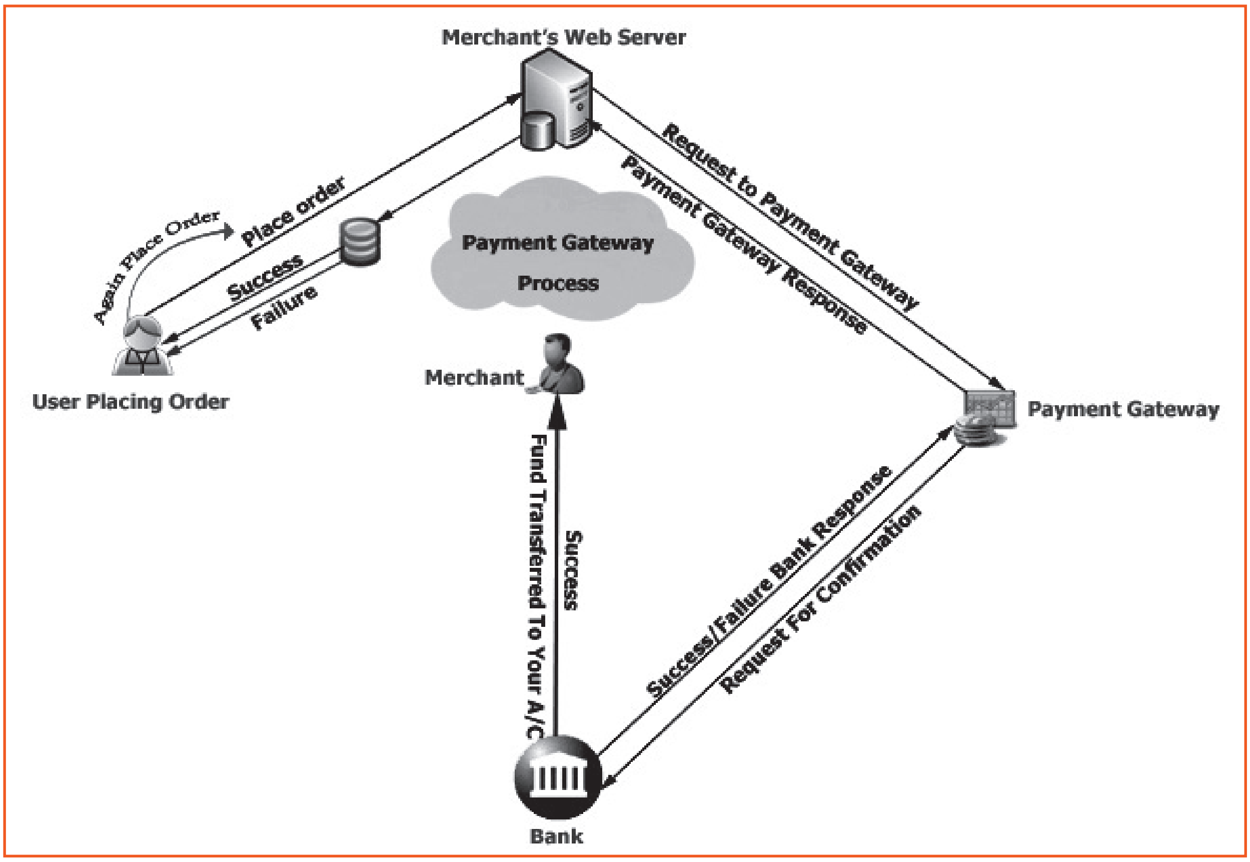


Fig. 11.2. Electronic Payment Gateways

*"The great secret of true success, of true happiness, is this: the man or woman who asks for no return, the perfectly unselfish person, is the most successful." - **Swami Vivekananda***

Once the customer places the order to purchase the goods or services on the vendor's portal, transaction details are sent from the merchant site which uses HTTPS application. HTTPS application means 'Hyper Text Transfer Protocol Secure'. The information is sent by the HTTPS application through a Security Socket Layer (SSL) application. SSL is a payment gateway security protocol used by the SSL server. SSL is a security layer that provides secure connection between the customer and merchant. It carries out encryption process by using two keys. The information provided by the customer such as the login details and personal information is encoded and sent to the recipient. The version is decoded and viewed by the recipient. The key to decode the information is known only by the recipient.

The HTTPS application along with SSL provides for encryption of the information transmitted which secures the network, the server and safeguards payments made online. SSL is a combination intended to provide encrypted information and secure identification of a network web server. HTTPS connections are used for sensitive transactions and secure the information transmitted to the payment gateway. A payment gateway thus affords a secure link between the merchant, customer and credit card processor.

The payment gateway assures that the credit card holder is credible and keeps the information secure and passes it to the processor for further transaction. The payment gateway forwards the transaction information from the merchant's website to the payment credit card processor used by the merchant's acquiring bank. The payment processor forwards the information to the Credit Card Interchange which is the organization responsible for processing, clearing and settlement of credit card transactions.

The Credit Card Interchange then routes the transaction to the customer's credit card issuer where it is either approved or declined depending on the balance available on the credit card. If the transaction is approved, the funds are routed back to the Credit Card Interchange which provides the merchant's bank processor with the transaction results.

The transaction goes back to the payment gateway which is responsible for conveying the approval/decline of the transaction to both the customer/card holder and the merchant/ e-commerce seller. At the end, the Credit Card Interchange sends the funds to the merchant's bank.

A payment gateway can be installed on the merchant's server. This would require the merchant to comply with all security measures of encryption. Housing the payment gateway allows the merchant to capture all customer information in the database. If the payment gateway is housed by a third party, the customer information and details are not at the disposal and tracking chargeback can be difficult for the merchant. However, the merchant site should provide all possible security measures to keep customer information secure.

In addition to the existing security systems (HTTPS and SSL), new security codes are being introduced worldwide in order to enhance security levels. These new systems include 1) 3D

Secure Protocol/Virtual Payer Authentication (VPA), 2) IP Address and Address Verification System (AVS), 3) Card Verification Value (CVV), PCI and SET.

11.1.3 3D Secure Protocol / Virtual Payer Authentication:

VISA 3D Secure Service is known as 'Verified by Visa' and provides PIN protection when using a VISA credit card on the internet in order to make online payments more secure. This is an XML-based protocol developed by VISA which has been licensed to the other credit card companies. It is used by MasterCard as MasterCard Secure Code and has been selected as the standard for global, interoperable, authenticated payment.

The VISA 3D Secure works as follows. The security card holder is required to be registered in the 3D Secure system and will be issued a secure code with a password. When the credit card issuer has verified the responses, the cardholder will be enrolled and the verification information is stored on the Access Control server. Thereafter, every time the cardholder makes a purchase using his/her credit card with a participating merchant, a VISA 3D Secure request is generated by the merchant. The cardholder has to type in the PIN and the enrolment information stored on the Access Control server will be used to verify the cardholder's identity. If there is a mismatch, the server will reject the information as invalid and the payment will be declined. However, in order for this facility to be used by the customer/cardholder, the merchant's website has to make the necessary provisions for pop-up windows - For which they have to pay a setup fee, monthly fee and fee for each transaction. Nevertheless, Visa 3D Secure promises to alleviate some of the problems facing online merchants, like the distance between the seller and the buyer and customer identification.

11.1.4 IP Address & Address Verification System (AVS):

Address verification system (AVS) has been developed to check whether the address given by the buyer matches with the one on record for the credit card used. This system helps in verifying the address of the person holding the card. The billing address is checked with address provided with the card company to authenticate the user. Installation of IP firewalls by the merchant account service providers can prevent credit card fraud.

11.1.5 Card Verification Value (CVV), PCI and SET:

The Card Verification Value (CVV) is by now familiar to all credit card owners. It is the three digit code that is calculated from the data on the magnetic strip on the reverse side of the card and cannot be forged by simply knowing the credit card number. For the data information to be safe on a server, a hardware known as PCI (Peripheral Component Interconnect) which can be fitted to the motherboard of the computer should be used. In addition, SET (Secure Electronic Transaction), developed by VISA and MasterCard, provides for privacy and authentication of three parties thereby enabling secure transactions over insecure networks. SET provides for a dual signature wherein the dual signature containing the order information and payment information and sent to the merchant bank and the merchant. The dual signature is an encrypted message digest. The SET enables the merchant to view the payment information without obtaining access to the information itself.

11.2 Payment Gateways in India:

The selection of an appropriate payment gateway in India is particularly important for an e-commerce company as there have been many issues relating to both charges and reliability. There are two main choices for a start-up e-commerce company in selecting a payment gateway: one is a third party service provider and the other is a bank itself providing its own payment gateway.

Generally, a start-up e-commerce company will select a third party service provider while a large company will select a bank as a payment gateway. The third party players have low set up fees but can charge TDRS (the percentage money the gateway charges per transaction) up to 7% and is never lower than 2.5%. A larger, more established e-commerce company, that is a higher volume player, should select a bank as a payment gateway as they have lower TDRS and could offer a TDR lower than 2.5%. However, if the e-commerce company is only trading in some volumes then using a bank will become expensive.

Generally speaking, the payment gateways do not negotiate with smaller e-commerce companies who are, as a result, forced to accept their contracts as is where is. However, the e-commerce companies should take into consideration the issue of currency and whether the customers purchasing goods and services at their site will prefer to pay in INR or USD. The e-commerce company has to check whether the payment gateway supports transactions in Indian Rupees or only in USD and whether the gateway will add a currency conversion charge. Indian consumers are unlikely to purchase goods and services online in USD, therefore, it is important to find a gateway that will support payments in INR. Ideally, the payment gateway should support payments in both currencies so that overseas customers can pay in USD and Indian customers can pay in INR.

The Reserve Bank of India (RBI) was expected, in consultation with the National Payment Council, to work on the Payment Systems Regulation Act. This Act would presumably have regulated settlements through electronic payment gateways, stock and commodity exchanges and clearing houses. Notably, the IT Act does not apply to negotiable instruments which would limit its jurisdiction over electronic payment mechanisms.

11.3 Security Issues:

The main security issue in e-commerce is online credit card fraud, that is, obtaining money from another's account without authorization. The credit card details obtained without authorization are used for withdrawal of funds from unauthorized accounts, fraudulent purchases, and obtaining false credit.

Credit card fraud is perpetrated through hacking, skimming, identity theft, phishing, card being stolen, Cardholder Not Present (CNP) transactions and pharming as discussed below. Credit cards are vulnerable to fraud because, once the online purchase transaction is over, the credit card details are still stored on the network, database or other storage devices which are not secured and are prone to hacking. A hacker may infiltrate the network using a virus which attacks the server on which the information is maintained. Credit card details could also be obtained from the network or server if they are not protected from the use of malicious software. The bulk of credit card fraud cases in India take place in cardholder not being present (CNP) circumstances and, of course, all e-commerce/online transactions are CNP transactions. However, before examining CNP, we address how credit card fraud is perpetrated through hacking, skimming, identity, theft, phishing and pharming. Although these types of Cyber Crimes have already been discussed in Chapter 1, they are examined here in the context of credit card fraud.

11.3.1. Hacking:

A hacker need not know the entire details of the cardholder in order to be able to make unauthorized use of someone's credit card because details may be available elsewhere on the web. Once the hacker knows a person's credit card number, he could obtain the cardholder's date of birth or address from social networking sites. There are various methods of obtaining credit card details and information.

11.3.2 Skimming:

Electronic method of capturing a victim's personal information used by identity thieves. The skimmer is a small device that scans a credit card and stores the information contained in the magnetic strip. Skimming can take place during a legitimate transaction at a business.

Skimming is the process of capturing personal information on the credit card by using a skimming device to scan the card details on the magnetic strip. The numbers on the magnetic strip are erased and a new number is embossed and transactions are carried on using the new numbers. A magnetic strip contains the card holder's name, 16 digit credit card numbers, an expiration date and a creditcard verification value (CVV). This information available on the magnetic strip is sufficient enough to make a card similar to the original one. This makes the magnetic strip more vulnerable to theft. When the card on which the new number has been embossed does not work in the swiping machine, the merchant manually processes the details of the card to complete the sale. Therefore, the transaction is completed even though the numbers on the original magnetic strip have been erased and a new number has been embossed.

Unlike a magnetic strip, a credit card chip on an RFTD transponder provides additional security. A new CVV is generated for every transaction which is completely different from the one in the card. The new CVV is communicated to the network for it to be used for the new transaction. In this case, the information on the card cannot be skimmed as a new CVV is generated for every transaction.

11.3.3. Phishing:

Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal your personal information. They send out e-mails that appear to come from legitimate websites such as eBay, PayPal, or other banking institutions. The e-mails state that your information needs to be updated or validated and ask that you enter your username and password, after clicking a link included in the e-mail. Some e-mails will ask that you enter even more information, such as your full name, address, phone number, social security number, and credit card number. However, even if you visit the false website and just enter your username and password, the phisher may be able to gain access to more information by just logging in to your account.

As discussed in the introductory chapter, Phishing is another method to obtain user- names and passwords of credit cards or bank accounts under false pretences. Phishing is a type of internet scam where the spoofed e-mail message is, for example, sent on the pretence of updating or verifying information of the account. A link from the spoofed e-mail leads to a fake website resembling the original website, which is a forgery. The customer unknowingly provides all the information to the false website, which purports to be the real website of the bank or credit card company, and the fraudsters thus obtain the information needed to hack into the user's bank accounts, transfer funds, etc There are various mechanisms available to prevent phishing. In order to prevent phishing, a merchant should use spam filter software, antivirus software and personal firewalls.

In addition to sending spoofed email messages or text messages, malicious software is used by fraudsters as an email attachment to search for personal banking information and passwords kept on a person's computer and some worms hijack the users host file which directs it to a fake phishing website.

Another method of phishing involves the use of spyware which is planted on a user's computer and the information obtained is redirected to the fraudster's computer network. Yet another method of phishing is called 'tab nabbing' where a third party script is downloaded and is transformed to appear like a bank account, email account etc In order to avoid these spoofed emails/websites, it is advisable that credit cardholders should directly access their bank's website through the particular bank's URL.

11.3.4 Pharming:

Pharming is yet another way hackers attempt to manipulate users on the Internet. While phishing attempts to capture personal information by getting users to visit a fake website, pharming redirects users to false websites without them even knowing it. While a typical website uses a domain name for its address, its actual location is determined by an IP address. When a user types a domain name into his or her Web browser's address field and hits enter, the domain name is translated into an IP address via a DNS server. The Web browser then connects to the server at this IP address and loads the Web page data. After a user visits a certain website, the DNS entry for that site is often stored on the user's computer in a DNS cache. This way, the computer does not have to keep accessing a DNS server whenever the user visits the website.

Pharming is another method of obtaining the PIN codes, access numbers and other confidential information required to perpetrate credit card fraud. Pharming occurs where the hackers redirect the website traffic to another i.e. a fraudulent site. This can be done by changing the host file on a victim's computer or attack the DNS server's software, i.e. Domain Name System, (which is the name of computer connected to the internet) through introducing a virus or malware. By introducing a virus/malware into the victim's computer, the fraudster is able to redirect the victim to a fake/scam website which might appear like the original website which is called page-jacking. In other words, the URL entered in the browser by the victim redirects to a fake address. The fake website would ask for sensitive information like the user name, passwords, and credit card details. Anti-spyware or antivirus can be used to protect against a host computer being attacked by a virus or malware.

11.3.5 Cardholder Not Present (CNP) :

As discussed above, most of the credit card fraud in India occurs when the credit card is used when the cardholder is not present (known as CNP). A CNP transaction occurs for all e-commerce transactions as these are all online purchases and not physical purchases where the cardholder is present in the shop. In fact, neither the card nor the cardholders are physically present at the time of carrying out an e-commerce transaction. If the cardholder is not present at the time of executing the transaction, it is less clear whether it is the actual cardholder or a fraudster who is carrying out the transaction.

The credit card fraud in a CNP is perpetrated by skimming or through other methods discussed above such as pharming, phishing or, identity theft. Through one of these methods, the credit card details, access codes/PINs are stolen from the network or server or from the magnetic strip of the card etc When an unauthorized user carries out the transaction, the merchant is unaware who is carrying out the transaction.

As discussed above, various security measures are available to establish whether the person is providing a credit card detail is an authorized user. The merchant should request the credit card number, cardholder's names and details, secure code provided by issuing bank, secret code, Virtual Payer Authentication, and AVS where the address on the credit card is verified with the address provided in the file of the issuing bank. The three digit number, that is, the Credit Value Verification (CVV) should be checked by the merchant when an order is placed.

There are various circumstances when card holder not present fraud can be expected, i.e. when multiple account numbers result in shipping goods to the same address, transactions with similar account numbers, multiple transactions on one card in a short period, multiple account numbers from the same IP address. Frequent attempts to find the number can alert the issuing bank and thus they may not be successful. The company carrying online business should ensure the use of AVS, CVVs, Virtual Payer Authentication and other security measures as discussed above.

In an attempt to curb credit card fraud, the Reserve Bank of India (RBI) has set up a Credit Information Bureau of India in collaboration with Dun and Bradstreet (D&B).

However, credit card statements should be checked on a monthly basis. The RBI has issued a circular entitled 'Credit Card Operations of Banks' requiring banks to have internal control systems to prevent credit card fraud. The RBI has advised the credit card issuing banks to check 'know your customer' requirements in detail.

11.4 Taxation of E-Commerce:

In any jurisprudential system, taxing statutes are enacted for a social purpose. To the mind of the author, taxation is an exercise in pursuance of deriving collective solutions to individual problems. Revenue generated from taxation, helps the state to perform multifarious functions and provide security and stability to the economy.

Mobilization of financial resources through taxation has a substantive impact on the functioning of the economy. Though the statutory provisions governing taxation establish the basic principles, there exist uncertainty in several aspects. The author intends to discuss one such thought-provoking issue under the Income Tax Act, 1961, namely, can the principles of preventive detention be invoked and applied by the income tax authorities to detain a tax-payer.

E-commerce changes the nature of the physical requirements necessary to do business. The fact that the location of the business, the place where the transaction is initiated, the place where the goods and services are delivered and the server through which payment is made are usually all virtual challenges in traditional theories of taxation. The absence of a physical presence makes it difficult to apply traditional principles of taxation relating to the residence of the parties or source of the income known as residence based taxation or source based taxation. Residence based taxation means that all individuals and legal entities are subject to tax in the place where they are resident. Source based taxation means that all income may be taxed by the country which is the source of the income.

Furthermore, basic principles which apply to cross-border taxation should necessarily also apply to e-commerce transactions which are inherently cross-border. The fundamental principle is that when a resident of one country earns income from economic transactions in another country, both countries have a right to tax the same income. The home country has the right to tax the income on the basis of the residence rule and the other country, the host country, has the right to tax the income on the basis of the source rule of taxation. This gives rise to the problematic of double taxation which is addressed in the various bilateral Avoidance of Double Taxation Treaties.

The next section examines some of the basic principles of taxation under Indian law to ascertain whether they may be relevant to taxation of e-commerce transactions.

11.4.1 Principles of Taxation under Income Tax Act, 1961:

Under Indian Tax Law, Indian residents are taxed on their worldwide income whether or not it accrues, arises or is received inside or outside India. Non-residents are taxes on their income which is from a source in India.

Under Section 9 of the Income Tax Act, 1961, all income accrues, arises or is received which is deemed to accrue or arise in India is taxable in India.

11.4.2 OECD:

The OECD Model Convention provides for fair practices in e-commerce business. In January 1999, the OECD Committee on Fiscal Affairs constituted the Technical Advisory Group on Monitoring the Application of Existing Treaty Norms for Taxing Business Profits (TAG). The mandate of TAG was to examine how the current treaty rules for the taxation of business profits apply in the context of electronic commerce and examine proposals for alternative rules. The TAG focused on a) the 'place of effective management', b) the concept of a Permanent Establishment (PE), c) the attribution of profit to a server PE, and d) Transfer Pricing.

11.5 Foreign Investment in E-Commerce:

As per the Consolidated FDI Policy published by the Department of Industrial Policy and Promotion, Ministry of Commerce & Industry on October 1, 2011, E-commerce activities refer to the activity of buying and selling by a company through the e-commerce platform. As per the Consolidated FDI Policy, such companies would engage only in Business to Business (B2B) e-commerce and not in retail trading, implying that existing restrictions on FDI in domestic retail trading would be applicable to e-commerce as well. Under Indian Law, only up to 51% foreign investment is allowed in the retail sector provided the shops sell a single brand. Foreign investment in retail shops which carry multiple brands, referred to as multi-brand retail trading, are prohibited.

Provided the E-commerce activity is on a B2B basis, then 100% foreign investment is allowed on the automatic route. This means that prior approval is not required from the Foreign Investment Promotion Board (FIPB) in the Ministry of Finance and the foreign investors can directly proceed with incorporating the company in India.

अध्याय 12
Chapter 12
Cloud Computing

Notes :

12.1 Introduction:

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as the cloud) is used as a metaphor for the Internet, so the phrase cloud computing means a type of Internet-based computing, where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet.

Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnessed to solve problems too intensive for any stand-alone machine. As learned from past events, computing in its purest form, has changed hands multiple times. First from near the beginning when mainframes were predicted to be the future of computing. Indeed mainframes and large scale machines were built and used, and in some circumstances are used similarly today. The trend, however, turned from bigger and more expensive, to smaller and more affordable commodity PCs and servers.

Most of our data is stored on local networks with servers that may be clustered and sharing storage. This approach has had time to be developed into stable architecture, and provide decent redundancy when deployed right. A newer emerging technology, cloud computing, has shown up demanding attention and quickly is changing the direction of the technology landscape. Whether it is Google’s unique and scalable Google File System, or Amazon’s robust Amazon S3 cloud storage model, it is clear that cloud computing has arrived with much to be gleaned from.

In dealing with the abstract term, “the cloud”, it is easy to misunderstand what makes up the structure and function. The basic function is what comes from “the cloud”. Input is what makes the cloud tick. Do not confuse cloud computing with the term data centre, as it typically sits on top of the latter. Viewing the cloud as logical rather than a physical, you can see it object describes it better.

As new technologies emerge, they often tend to build on the success of previous developments. Cloud computing and storage, benefit from years of development and testing of large scale infrastructure. The most important take away is cloud storage is for everyone and every organization. From big to small, groups to individual, the use of grid infrastructure can be deployed for maximum return and efficiency.

The ‘cloud’ is a metaphor for the internet itself. Every time a person uses the internet to search any term on Google or use their web-based email services to send or receive emails, he or she is using a cloud application. A person who uses Facebook or other social networking sites is using a cloud application. In fact, when the internet was first being developed, file sharing, hosting services and email itself were the first cloud applications. Therefore, every person who has ever surfed the internet or used Hotmail or Google mail has already used the cloud. Nevertheless, despite the concept of the cloud being nothing new, ‘cloud computing’ is revolutionizing the way in which the world is computing data.

Cloud computing means using the internet and central remote servers to maintain data and applications instead of maintaining data on individual mainframe computers or PCs. This means that a person could click on the start menu of any computer anywhere and access all his files as though he was using his own desktop or laptop computer. As a result, a person could work on anyone's computer with the same ease as though he was working on his own computer in his own office. The files appear to be loaded on the hard drive of that computer while infact they are not located on that computer and have been downloaded from the cloud/internet onto that computer.

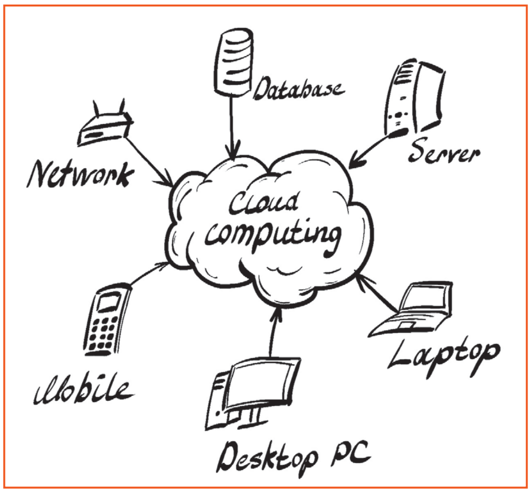
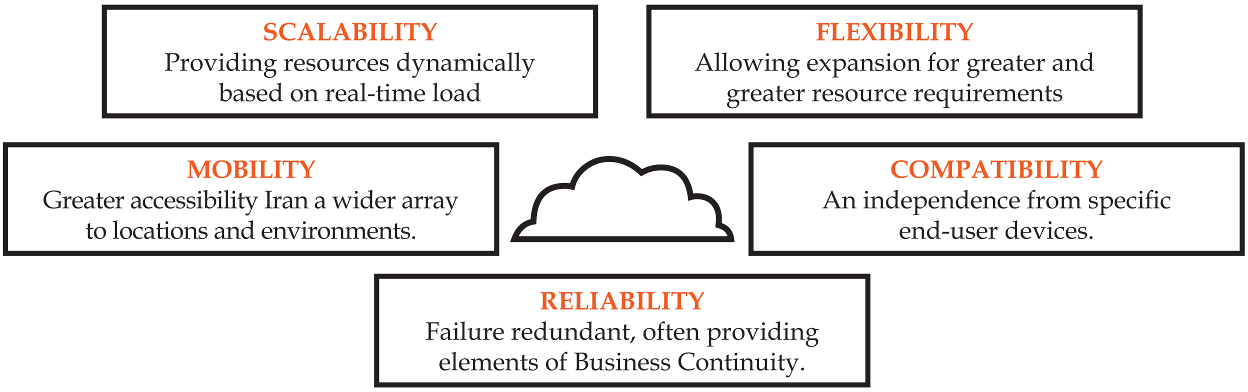


Fig. 12.1. Cloud Computing Applications

Cloud computer is enabled by a highly available, reliable pool of computing resources which can be paid for as a service and which replaces the need for mainframes, hardware, software and other IT infrastructure. Put simply, cloud computing has turned IT infrastructure into a service. As aptly described by commentators, cloud computing has turned software and computing into a utility in the same manner that electricity or water supply is a utility. Cloud computing has transformed the use of computing resources from a mainframe system or PC maintained by an individual user into a metered service in which users pay for what they use just like electricity or water is a metered service. Cloud computing has therefore transformed the computing and storage of data by replacing large, up-front capital investments in IT infrastructure with much lower, pay-per-use payments to cloud service providers.

The financial and availability benefits of cloud computing are immediately obvious. By using cloud computing services, companies no longer have to make the large, up-front capital investments in hardware, software and other IT infrastructure. As a result, businesses save the considerable costs of maintaining their own hardware infrastructure and servers and purchasing software licenses. Companies can also access their data more cheaply as the cloud centralizes storage, memory, processing and bandwidth thereby necessarily reducing costs and allowing users to benefit from economies of scale.



SCALABILITY
Providing resources dynamically based on real-time load

FLEXIBILITY
Allowing expansion for greater and greater resource requirements

MOBILITY
Greater accessibility Iran a wider array to locations and environments.

COMPATIBILITY
An independence from specific end-user devices.

RELIABILITY
Failure redundant, often providing elements of Business Continuity.

Fig. 12.2. Cloud Computing Benefits

Benefits of Cloud Computing:

Since cloud computing is a scalable, metered service, a user can quickly ramp up when it has high demand for computing resources and scale down when demand drops and thereby incur lower costs. In contrast, a company which has made the capital investments in IT infrastructure has incurred the initial costs, must pay recurring maintenance costs and cannot scale down if its own computing requirements decrease. Companies can increase their profit margins as the cloud lowers operating costs, provides easy mobility and better storage systems of the data. In short, running applications purchased from a 'cloud' is much more efficient and cheap than running one's own computer systems and applications.

Cloud computing allows consumers and businesses to use applications without installation and access their personal files stored online. Earlier, various software applications had to be installed on a single system. With the advent of cloud computing, a single application provides the user with access to a web-based cloud which hosts all the programs necessary to accomplish word-processing as well as all the other computing needs of a person. A cloud user will never have to face the loss of data because the hard drive of his PC has crashed or software has been corrupted. If a cloud subscriber's PC fails or is stolen, the subscriber only has to download his data from the cloud and will not even have to restore the files from back-up or otherwise try to restore his data from his PC.

In short cloud computing refers to the technologies that provide software, data access, storage devices that do not require physical location of the system. The main advantage over the conventional forms of applications is that cloud computing need not depend on a physical structure for its operations. A very interesting feature of cloud computing is that, as mentioned above, interoperability of various interfaces is imperative. Accordingly, the development of cloud computing will necessarily promote the growth and use of open source software.

12.2 Types of Clouds:

There are three main models of cloud computing: the public cloud, the private cloud and the hybrid cloud.

12.2.1 Public Cloud:

A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the Internet. A public cloud is owned by the provider selling cloud services and is external to the user's organization. As discussed below, a public cloud creates the greatest risks in terms of data security in that anyone who subscribes to the cloud has access to it. A public cloud is 'multi-tenant' in nature as the data of one company is necessarily stored along with the data of another company on the public cloud, therefore, data segregation is a very important issue.

12.2.2 Private Cloud:

A private cloud (also called internal cloud) is one in which the computing environment is operated exclusively for a particular company or organization.

The private cloud provides services to a limited number of users behind a firewall.

The private cloud can be managed either by the organization/company itself or a third party and may be hosted within the organization's data centre or outside it. The private cloud is reminiscent of an intranet, access to which is limited to the personnel of a particular company or organization. A community cloud is similar to a private cloud except that it is used by two or more organizations.

A private cloud is usually used by a large company and it offers various applications to upgrade or downgrade the resources as required by them. The private cloud of course does not offer the basic advantage of cloud computing because the user still has to incur the up-front capital costs in creating its own private cloud, however, these costs should be less than the costs incurred in creating its own traditional IT infrastructure over the long term. Moreover, the use of a private cloud means that the user is making more efficient use of assets instead of installing traditional IT infrastructure. Furthermore, operating expenses will be reduced due to lack of the hardware and other IT infrastructure when setting up a private cloud. The metering capabilities of the cloud is also expected to increase transparency in the business process. In addition, the private cloud provides the benefits of increased flexibility in that the user can ramp up and order services when needed.

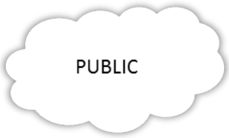
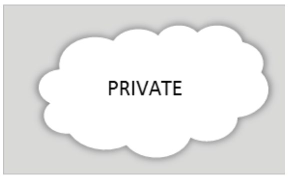
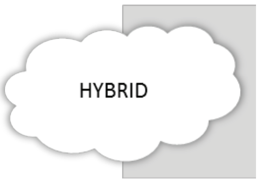
	Users	Characteristics
	Organizations or Individuals	Public clouds are the most common and can be used by organizations and individuals. There are around 100 million users on the public cloud. Anyone can access well-known public cloud services via the Internet. Well-known examples are Google applications or Amazon Web Services.
	Organizations	Private clouds are mostly used by organizations. It provides more control and more safety of the data as it is hosted on site rather than on external servers. A private cloud can be accessed on the web, but the data is secured and controlled behind the organizations firewalls. SUNGUARD, rackspace and terremark, among others, provide these types of private clouds.
	Organizations	Hybrid clouds are a fast growing type of cloud. They are connecting private clouds and public clouds. The benefit is to access public cloud services while ensuring the safety and control of a private environment. The sensitive data can be hosted on the private side while enabling access to features on public clouds. Thus, the Hybrid cloud is a way for IT to keep control over sensitive data, while answering users demand for public cloud services.
	Organizations	Community clouds are a private form of clouds, yet shared by multiple organizations in an industry. They are limited to defined users who share common resources. For example, Clinovo provides community cloud-based hosting clinical application services for its clients.

Fig. 12.3. Public, Private, Hybrid and Community Cloud

12.2.3 Hybrid Cloud:

A hybrid cloud is a composition of two or more clouds (private or public) that remain separate cloud entities but share certain technology which permits interoperability. One type of hybrid cloud is called 'cloud bursting' that is where a service provided by a private cloud can automatically access and use resources from a public cloud when it needs to ramp up and handle peak demand. The hybrid model means that companies can extend their private cloud network to the public cloud service providers.

12.3 Service Models:

There are three main service models, that is, types of services offered by cloud computing providers: Infrastructure-as-a-Service, Software-as-a-Service and Platform-as-a-service are the frequently used cloud service models.

12.3.1 Infrastructure-as-a-Service (IaaS):

'Infrastructure-as-a-Service' (IaaS) is the sale of hardware, storage and network as a service. Infrastructure-as-a-Service (IaaS) is the most basic model it involves providing only basic storage and data hosting. IaaS is provision of the basic computing infrastructure of servers, software and network equipment as an on-demand service upon which a platform to develop and execute applications can be established. The advantage provided by IaaS is that the subscriber/user does not have to purchase, house and manage the basic hardware and software infrastructure components and can obtain these resources from the service provider. The subscriber can choose the operating system and development environment. IaaS is becoming increasingly attractive because data storage requirements are increasing exponentially as a result of increasing connectivity of industrial and other infrastructure to the Internet.

12.3.2 Software-as-a-Service (SaaS):

The second model is SaaS. In this model, the cloud provider provides the software to access, manage and utilize data. An example of SaaS is email service providers such as Gmail, Yahoo mail, Hotmail and social media sites such as Facebook, LinkedIn and Twitter. SaaS means that one or more applications and the computational resources to run them are provided for use on demand as a turn-key service.

The advantage of SaaS is that it reduces the cost of hardware, software development and maintenance for the user/subscriber. The subscriber does not manage the cloud infrastructure or individual applications and may make only some limited administrative application settings. Prior to the advent of cloud computing, users had to purchase licenses to use software applications. Cloud computing has now transformed software into a service. Instead of purchasing the software, the user pays for use of the cloud facility which provides the software applications.

12.3.3 Platform-as-a-Service (PaaS):

The third model is 'Platform-as-a-service' (PaaS). PaaS is the sale of an application development platform as a service. An example of PaaS is Facebook allowing third parties to build and distribute applications within its service.

PaaS is the provision of a computing platform as an on-demand service upon which applications can be developed and deployed. PaaS provides the tools to develop applications in a standard environment allowing new businesses and applications to be developed faster with less risk. The PaaS model is intended to do away with the cost of buying, housing and managing the hardware and software required for the platform. However, the subscriber has control over application and the application environment settings of the platform.

12.4 Cloud Computing and India:

According to reports, India has a population of 8 million small-to medium-sized businesses which are potential users of cloud computing services. The Indian cloud computing market was estimated at $66.7 million (around Rs. 300 crores) in 2009 and is expected to grow at a compounded annual growth rate (CAGR) of 40% over the next five years. According to the IDC's India Cloud Computing Market — Current State and Future Roadmap Study, 2010, cloud computing is expected to rise to 6.8% of large and mid-size enterprises by 2012. The Indian cloud market is expected to become a $3 billion market by 2015. According to a Gartner survey, two-thirds of Indian CIOs expect the majority of IT to be running in the cloud within the next four years.

The advent of cloud computing in India is expected to attract additional foreign investment. The availability of good operating systems, data storage facilities and lower costs are expected to prompt foreign companies to establish a base in India. Many Indian companies, particularly in the telecommunications and healthcare sectors, have adopted the hybrid cloud model. However, in India, there are particular challenges hindering the development of computing such as the lack of reliable supply of electricity and internet access.

12.5 Legal Issues:

Cloud computing raises a number of legal issues. Since cloud computing involves storing and processing huge amounts of information in the cloud, it raises complex issues of data security and privacy particularly in a public cloud as the data of various companies are all stored together in the same cloud. It is important for the service providers to provide the customers with encryption codes to protect the information on the cloud. Data portability between service providers is another major issue.

Second, cloud computing raises serious issues regarding Cyber Crime and hacking because a cloud environment is not a traditional secure network. Instead, it is an environment in which any user/subscriber can gain access and use. This means a hacker may pose as a user in order to introduce bots or other malware into the cloud.

Third, cloud computing raises issues concerning protection of intellectual property rights. The threshold question is who owns the data stored in the cloud? The immediate response is that the IPR in the work stored on the cloud would be owned by the subscriber. However, in a cloud, information is constantly being added, removed or modified and new information created. Therefore, it is important to specify that the subscriber owns all the IPR in the compilation of information created in the cloud.

Cloud computing also raises complex issues regarding jurisdiction. As discussed in Chapter 11 on E-commerce, a key element determining jurisdiction is physical location. The general norm includes a house computing centre allowing the enterprise to know where the data is located and the methods of securing the data on the cloud. However, sometimes the service providers do not disclose the location of the data. Issues arise when the data flows to another jurisdiction. Often, even the providers of cloud computing services do not know exactly where the data is located. The data may be located in several countries which gives rise to vexed questions relating to jurisdiction. This chapter examines issues relating to data security and privacy as well as Cyber Crime in the context of cloud computing.

12.6 Cloud Computing and Cyber Crime:

Cloud computing is not a traditional secure network on the internet where access from outside the network can be completely prohibited. Instead, in the case of cloud computing, any subscriber with access from outside the network can login to a public cloud as long as they have internet access. Security is a major concern because data is not locked in a secure location. Instead, data in the cloud shares computing resources with others' data and if not secured properly can be accessed by cyber criminals.

According to reports, the increased use of cloud computing technology by companies has led to a significant increase in attacks on companies that use virtualized and cloud based environments. Hackers have reportedly been targeting companies utilizing web-based applications used to store sensitive financial, employee, corporate and medical information targeting them with web-based intrusion attacks. According to the Trend Micro 2010 Future Threat Report, 'cloud computing and virtualization move servers outside the traditional security perimeter and expand the playing field for cyber criminals.' Danger/Sidekick's cloud based server failure caused major data outages in November, 2009 which evidenced the risks that cyber criminals will take.

As information goes through the system of a public cloud, cloud risks increase and, once you release the data, it is nearly impossible to control where it goes later. Moreover, large companies are unlikely to report attacks on the cloud. Encryption is also not a sure method of avoiding problems. Issues will arise as to who holds the key for the encryption. Further, decryption may be required if the data is processed in the cloud.

Some progress has been made with the advent of technological improvements. The hardware and virtualization layers were formerly an inscrutable 'black box.' Now, these layers can be inspected, analyzed and reported on for compliance in the same manner as the cloud's top-most application services layer. There are also new data privacy technologies such as encrypted volumes, point-to-point secure communication and secure database transactions which are the new security mechanisms that would secure cloud data platforms.

12.7 Conclusion:

Cloud computing is a paradigm shift in the internet age and is revolutionizing how technology is delivered. However, the advantages in terms of costs, flexibility and availability enjoyed by the users of cloud services also bring with them new challenges against Cyber Crime, data security, protection of intellectual property rights and jurisdictional issues. Indian legislators and the courts have yet to react to the new phenomenon of cloud computing, therefore, this is a space to watch in the near future.

अध्याय 13
Chapter 13
Digital footprints – Assessing Computer Evidence

Notes :

13.1 General:

Did you know that everything you do online leaves a trace? It's true. It's called a digital footprint, and while it may seem invisible to you right now, other people can see it, including your friends, family, your future college or employer, and even companies that want to sell you something. Think about what you have done so far today. If you checked Facebook, Tweeted, left a comment on a message board or blog, or even just visited a website (including this one), you've shaped a piece of your digital footprint. While you watch the video below, created by Common Sense Media, think about the ways you and your friends are building your digital footprints every day. Then, go to Follow Your Footprint to learn more about your online practices.

What Makes Up Your Digital footprint?

Your personal information: name, address, phone number, birthday; Your actions and uploads: texts, photos, sites you have visited, things you say and things others say about you online; Your digital trail, which may be invisible to you: Data collected about you from using your TV, telephone, cell phone, Internet, and other tools that you use in your everyday life. Often this data is used by companies for marketing purposes.

How You Create Your Digital footprint:

How much do you think about and value your privacy? You might feel upset if a parent or sibling went into your room without permission, or checked up on your Facebook profile. But, in a world where everyone is connected and anything created online can be copied, pasted, and sent to thousands of people in a heartbeat, privacy starts to mean something different than simply guarding personal or private information (Common Sense Media, 2009). So while you might think a lot about privacy as it relates to the people you know, you should consider that when every time you update your status on Facebook, tweet, comment on something, post a video, or text a friend, you are making a decision about your privacy as it relates to a lot of people you've never even met. You are creating your digital footprint every day. You make decisions online every day that may seem short term, but could have long term consequences, long after you've forgotten what happened today. Have you ever posted something online that a friend passed along or re-posted in a way you didn't anticipate? Have you ever re-posted something that belonged to a friend without asking them first? Or put real life business, like a fight or a break up, online? Who is reading the messages on your Facebook wall? You may think that only your friends would read about it or care, but an adult (such as a college admissions counsellor or hiring manager) might see it and think twice about you. Everything leaves a digital footprint. Whatever gets created may never go away. If they don't want to see it tomorrow, they'd better not post it today (Common Sense Media, 2009).

What is Digital Citizenship?

Who is a digital citizen? You! A digital citizen is anyone who uses digital tools such as computers, cell phones, or the Internet. You can use these tools in your work, at school or for recreation. Similar to how rules and standards of behaviour exist for citizens of a city, those of us in the digital world should also follow rules and policies (Computer Applications, 2010). Digital citizenship is everyone's responsibility. You have a responsibility to treat your digital footprint, and those of your friends with respect. Your friends are also responsible for treating your digital footprint with respect, and not to do anything that might hurt you now, or later.

Creating a Positive Digital footprint:

Your digital footprint is an online version of you! It may be the only description someone has about you, particularly potential employers. Here are some tips to make sure that view is positive. Google yourself or set a Google Alert. This will let you know when someone has posted something using your name. If you are graduating this year, create a LinkedIn account. Make sure that you have applied the Facebook privacy settings to limit who has access to your profile. Remember that we live in a digital world and digital content can be easily changed and accessed. Expand your online network. Connect to friends of parents, parents of friends, relatives and neighbours. Connect with adults likely to recommend you for a job.

Our digital footprint can impact:

- Our online reputation and image.
- Our real life reputation and image.
- Our employment prospects.
- Our admission to school, university or groups.
- Our relationships with friends, family, teachers and other people in our network.
- The reputations of friends, family, teachers and other people in our network.

Importance of Digital footprints:

This activity addresses the topic of digital footprint. Digital footprint is defined as "online portfolios of who we are, what we do, and by association, what we know" (Richardson, 2008). It is also known as our digital shadow, the footprints we leave after using internet based devices. Being aware of our digital footprint is not only important to us as professionals but it is important for the students to consider because it is very likely that their entire life has been documented online from their first baby photos to current activities they participate in today. Statistics from the Pew Internet & American Life Project indicates that 43% of online adults are unfazed and inactive when describing their level of concern about personal information online. These people do not worry about personal information online nor do they take steps to limit the amount of information. As educators, it is our responsibility to encourage students to consider their digital footprint and its lasting effects. This activity is designed to explain the concept of digital footprint and allow the students the opportunity to learn and inform others of how to protect their online.

13.2 Computer Evidence:

An expression that refers to the way technology now pervades everyone's lives, your digital footprint specifically describes the trail you leave in cyberspace and on any form of digital

"All power is within you. You can do anything and everything. Believe in that. Do not believe that you are weak; do not believe that you are half-crazy lunatics, as most of us do nowadays. Stand up and express the divinity within you."

communication. It is now widely accepted that in this era of e-mail, texting, blogging, and social networking, trying to hide one's digital footprint is practically futile. In fact, it's been reported that the FBI can hear your conversation via your cell phone even when it is turned off (the only thing to thwart this is take out the battery).

Computer evidence used to mean one of two things. Its most typical form was regular print-out from a corporate computer. The alternative form was a reading from any single-purpose measuring or counting device which can be regarded as a mute witness free from human intervention, such as an intoximeter, a telephone call meter or a weighing machine. Overwhelmingly journal articles and legal textbooks have concentrated on issues of admissibility. In the case of regular computer print-out, the problems have been of the scope and circumstances of certification of proper working and notions of document and statement"—what may be referred to in short-hand as "Section 69 issues". In the case of the simple measuring devices the problem has been the limits of this area of interpretation of "real evidence".

But over the last decade the huge changes in the physical forms computers take, the range of applications, patterns of ownership, the ways in which they are used and the extent to which they can be interlinked across businesses and across the world have produced many new forms of computer-derived evidence. Many of the assumptions in the earlier articles and in the precedents to which they refer are no longer true. For example a computer is not necessarily "just like" a filing cabinet and as a result computer "documents" may not be "just like "the paper equivalent. Again, it is not necessarily the case that computer errors are nearly always manifest in that the result is either no read-out or print-out of any kind or gross nonsense. Depending on circumstances, a computer print-out can look plausibly correct but nevertheless be misleading or be misinterpreted. Increasingly too, the Courts are being presented with configuration, logging and other system files which would not normally be viewed by the ordinary computer user—indeed such a user may not even know of their existence—but which investigators and prosecutors are tendering as evidence of an accused's activities or intentions.

13.3 Consultation Paper and the Report:

In both the Consultation Paper and the Report, the Commissioners showed concern about some of the practical problems of assessing the reliability of computers and computer output, though their focus was on Section 69 of the Police and Criminal evidence Act (PACE). They gave the following main reasons for regarding that section as unsatisfactory that it fails to address the major causes of inaccuracy in computer evidence; that advances in computer technology make it increasingly difficult to comply with Section 69; that it is becoming "increasingly impractical to examine (and therefore certify) all the intricacies of computer operation", that the recipient of computer evidence may be in no position to satisfy the Court about the operation of the computer, that it is illogical that Section 69 applies where the document is tendered in evidence, but not where it is used by an expert in arriving at his conclusions, nor where a witness uses it to refresh his or her memory. In the Consultation Paper, the Commissioners quote Kelman and Sizer with approval: "with a large and complex computer system, it is doubtful whether a manager could have sufficient knowledge [to issue a Section 69 certificate] the computer malfunction or an act of unauthorized tampering might be almost impossible to detect by all but experts in the field." A little later, the Commissioners go on to remark; comments from judges to the effect that determined defence lawyers can and do examine the prosecution's computer expert at great length. The complexity of modern systems makes it relatively easy to establish a reasonable doubt in a juror's mind as to whether the computer was operating properly. We are concerned about smoke-screens being raised by cross-examination"

The Commissioners' conclusion was that it is not possible to legislate protectively with regard to computer evidence and that where there are specific reasons to doubt the reliability of a particular document generated by a computer these doubts should go to weight and not to admissibility.

In effect, the Commissioners are throwing all the harden of assessment onto the Trier of fact, which for more serious offences, will be a lay jury. If we agree that it is mistake to "legislate protectively" given all the potential problems of rigidity in interpretation, are there any broad tests for "reliability" we can offer? Should we consider Codes of Practice which might guide law enforcement officers and the Courts? Would these be enough? Many of the expressed worries about the use of lay juries in trials of complex fraud transfer very easily to situations where there are complex computer systems. Again, many of the problems of assessing novel scientific evidence, most recently considered in connection with DNA Evidence re-appear with renewed vigour.

13.4 The Growth of Computer Forensics:

Cyber Crime is an illegal activity committed mainly through the use of computer systems, the Internet, or misuse of data. Computer forensics is a fairly new and growing field in which experts collect, analyze, and present evidence gathered from computer systems for use in court cases involving some element of Cyber Crime. Evidence may include information gathered from wireless devices, data storage systems, and computer networks. Those interested in pursuing careers in this field may major in information technology, computer science, or forensics. Some schools are even beginning to offer bachelor's degree programs in IT with a focus specifically on computer forensics.

A few brief paragraphs of historical context-setting may be helpful in understanding how and why the techniques came into existence. Three or four key trends have distinguished the history of computing over the last fifteen years and particularly the last ten years; the main trends have in turn spawned many lesser ones and all have interacted with, and reinforced, each other. They are: the growth in use and power of personal computers; the move in the design of corporate computer systems away from the centralised monolithic mainframe towards a multiplicity of smaller but powerful machines which inter-work and inter-connect in a form usually called distributed processing; and the growth of networks, both private and, in the form of the Internet, globally public. All of these changes have had an impact not only on what computers can deliver to their owners but also in the types of evidence that may be found with them.

13.5 Personal Computers:

Personal computers are now a very common item in many houses yet in 1955, there were only 250 computers in use throughout the world. In 1980, more than one million personal computers had been sold and by the mid-1980's, this figure had risen to 30 million. How did this come about?

PCs have been used for non-recreational purposes for almost 20 years, and today the sub-1000 PC is more powerful than many business mainframes of 20 years ago. Unlike physically larger computers, they can be easily taken away in their entirety during the execution of a search warrant, as they are personal to an individual in addition to formal business documents; they are much more likely to hold informal material which could, for example, indicate intentions or hidden activity. As a result of the increasing complexity of PC operating systems and applications, PCs create many non-obvious files which improve system performance and allow recovery in the event of disaster; on examination these can be interpreted to show how the computer has been used recently. PCs are also the primary means through which the Internet is used for sending global e-mail and viewing information on the World Wide Web. The programs that provide these facilities also create substantial logging and other files on the PCs hard-disk which can subsequently be examined.

13.6 Distributed Processing:

Distributed processing accelerates processing by distributing the work to multiple computers that have been chosen to provide more processing power. You can submit batches of processing jobs to the Apple Qmaster distributed processing system, which allocates those jobs to other computers in the most efficient way (described in more detail in How the Apple Qmaster System Distributes Batches).

Distributed processing is way of designing systems which, in contrast to the use of a single very powerful central computer which both holds and processes all organizational information, is easier to design, faster, cheaper and more resilent. A number of smaller computers are linked together so that they feed one another with information and resources; some of the smaller computers may be quite specialized in nature—indeed they can include automatic teller machines, warehouse and manufacturing robots, and bar-code readers. Distributed processing has been common in larger organizations

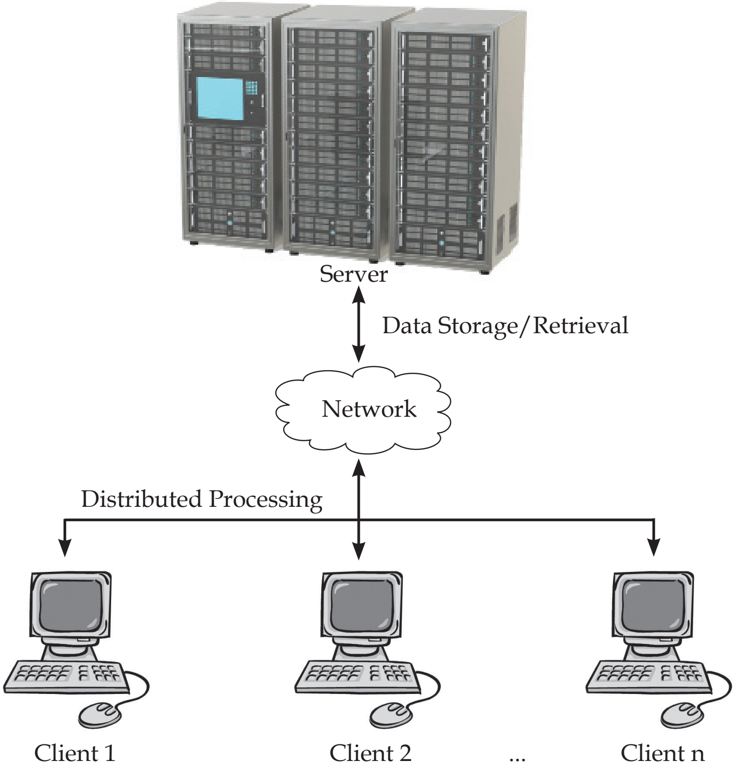


Fig. 13.1. Distributed Processing

for at least 15 years. From an evidential perspective, one consequence is that many computer documents are "assembled" only on demand and from many different sources. PCs are often used within distributed processing systems as the primary way in which executives see how the business is performing. Such PCs hold programs which interrogate the main system for information but display the results on the individual executive's PC in a way that the executive has personally devised. What appears on a screen or a print-out in these circumstances depends on the actions of the individual executive as well as the quality of the central pool of corporate information. The problem then is what someone seeking to rely on such a document must do to seize and produce it—and then be in a position to show it to be reliable for the purposes of "weight". Can one rely on a single print-out produced on one PC or should the entire corporate database be seized? Computer systems using distributed processing generate many intermediate and logging files, in addition, if care has been taken in introducing security measures, there may be yet other audit and logging files. Again a skilled computer analyst may be able to interpret these to provide assurance of consistency to a Court or alternatively demonstrate a critical inconsistency.

13.7 Networking:

When looking at networking basics, understanding the way a network operates is the first step to understanding routing and switching. The network operates by connecting computers and peripherals using two pieces of equipment; switches and routers. Switches and routers, essential networking basics, enable the devices that are connected to your network to communicate with each other, as well as with other networks.

In networks, where several computers are linked together, there are similar problems of discovering where a document is held and how much needs to be seized in order to provide sufficient "weight". There are a number of ways of designing networks; the simplest variety simply provides individual PCs with the capacity to communicate with each other and, depending on how the security is set, access part of each others' hard-disks. A more complex design would include one or more servers, larger computers which hold programs and data. The programs might include internal e-mail and the data may include back-ups of key business records. Servers are an important source of computer evidence. Distributed processing systems rely heavily on complex networks. In the largest of organizations, part of the network may be beyond local jurisdiction. Private networks also exist at an industry level and first-generation EDIs (Electronic Data Interchanges) depend on them.

13.8 Common Computer Forensic Techniques:

13.8.1 Seizure of Computer Hardware:

The purpose of this white paper is to teach you how to seize a computer from a crime scene. The techniques that you learn can also be used in non-criminal cases. For example, perhaps your job is to seize a computer from an employee who engaged in activities that go against the policies of your company. In either situation, it is imperative that you proceed with care to avoid tainting any evidence residing on the computer.

This is probably the best established of the techniques, and the one closest to traditional scene of crime activity. The protocols issued to the police describe a variety of investigative procedures, including carrying out a pre-raid intelligence review to assess what types of hardware maybe expected, what sorts of software, identifying what sorts of back-up might be held and how these might relate to potential evidence; defining the scope of warrants —this is not a forensic procedure as such but is essential if there is to be conformity with admissibility rules; photographing the computer(s) *in situ*, particularly any cabling of peripherals and ancillaries; careful identification and labelling of all items, including cables, peripherals, external data storage such as disks and tapes, careful dismantling, to include preventative measures to avoid inadvertent damage or contamination, and bagging; appropriate record-keeping; precautions to prevent the data being destroyed by hostile individuals immediately prior to the raid; the handling of computers that are running at the time of the raid; procedures for safe shutting down; the noting of the time on the computer's internal clock—which is used among other things, to provide date and time-stamps on computer files; and the making of an exact sector-by-sector copy of every hard-disk.

This last item needs some explanation. A particular problem of evidence from hard-disks attached to computers is that the very process of turning on a computer and/or seeking to copy its seeking to copy its contents can alter the contents to such an extent that they become contaminated. In order to avoid this most UK law enforcement agencies use a process sometimes called "legal imaging" which, with a combination of special hardware and software and appropriate procedures, is intended to overcome the hazards of contamination. The procedure should take place as soon as possible after a computer has been seized; subsequent examination is then carried out on the copies of the hard-disk. The method consists of starting (or "booting") the computer not from the first hard-disk as would be normal but from the floppy or drive. The computer is booted with a minimal operating system as opposed to a complex one like Windows 95. The operating system contains additional features or "drivers" which make the computer recognize an external data storage device such as a removable hard-disk. Still operating from the floppy drive, software is run which will make an "image" of the hard-disk (or hard-disks if there is more than one) onto the external device. The image is an exact copy (sometimes referred to as a "bit copy" or "sector by sector copy" of the original. It includes not only the visible files on the original disk but others which would normally not be seen, the parts of the disk that contain the information from which the directory details are obtained (file names, sizes, date and time-stamp) and also certain other forensic fragments from previously deleted files can sometimes be recovered. The "image" file itself cannot be viewed easily, but by reversing the imaging process onto a second computer similar in specification to the original, an exact clone of the original disk, including all the "hidden" information is created. This process is sometimes called "extraction". The procedures used have certain controls in-built; the original computer remains available for inspection; often two image copies are made, one to act as a control in a manner similar to that used where police-station interviews are taped. In addition, the images and the “extracted” files are recorded to CD-ROM, which is a Write Once, Read Many medium which cannot be altered. CD-ROMs made in these circumstances are usually disclosed to the defence. A further feature of the procedures as used by some law enforcement agencies is that, where ever possible, there is a separation between technicians who operate on the raw computer evidence and investigating officers involved in analysing the results. Essentially these protocols address the issue of freezing the scene. Witness statements and interview records are needed in support and to provide continuity of evidence.

Followed properly, hard-disk imaging is uncontroversial. From an admissibility perspective/ the computer and its hard-disk are “real evidence”; all subsequent images, copies, print-outs etc are “documents” and at the moment appear to need Section 69 certification. Problems arise from the types of material produced from the hard-disk and the inferences that may be made, for example :

- Simple data files—word-processed documents, database and accounts records, pictures, copies of fixes—produced from regular applications present little difficulty. The date-and-time stamp which can be displayed in the computer’s directory is of last modification rather than original creation. Some applications generate records of first creation and also list modifications, but most do not PCs do not normally create formal audit or logging records.
- E-mail messages and faxes, sent and received, may have been retained by the computer owner, but the owner may also have selectively deleted some of them.
- Sophisticated extended use of directory information can help build up chronologies of events within a computer, but the data available may be incomplete or imperfect and significant amounts of interpretation may be needed. The basic tool is to request a list of all files in all directories on all disks sorted in dated/time order. The chronologies may show, among other things: when an operating system was installed, reinstalled or upgraded, when an application was installed, re-installed or upgraded; when new hardware was installed or reinstalled; sessions during which files were being created or modified, sessions in which files were viewed without necessarily being modified; dates when faxes were sent and received; sessions online to the Internet and other external services; times when diagnostic packages were run because of some suspected system fault;
- Deleted files, particularly if the deletion is recent, can be recovered using facilities built into modem operating systems to provide resilence against accident. This is possible because initially unwanted files are only marked for deletion so that they do not appear in a disk directory though the content remains until the specific disk space occupied is re-used by newer files. This type of undeleting is uncontroversial, but technicians can also sometimes recover fragments direct from disk sectors; here a greater element of interpretation may be needed. Careful examination of certain application files, for example documents created in Microsoft Word, may include fragments which the creator believes has been discarded. The danger here is that a computer technician, in making a reconstruction of a document,

becomes influenced by other aspects of the investigation.

- Swap files are temporary files created on hard-disk by operating system when there is insufficient random access memory (RAM) for a specific activity, for example, when several programs run simultaneously, or a large document or picture is being edited. Here again a technician may uncover evidence of recent activities, including alterations and deletions to files, or the transmission of passwords. Here too one technician's interpretation may be challenged by another.

If an individual PC is handled properly at and after seizure and if it was within the sole control of suspect, a great deal of important evidence about the suspect's activities is potentially available. However some of the conclusions offered by prosecution experts may depend on interpretation rather than incontestable fact-finding, and the extent of this may not be obvious.

13.8.2 Larger Corporate Systems:

The larger the computer system, the greater the difficulties of transporting it anywhere, particularly if the system is extensively networked and consists of a number of disparate computers, linked together by networks for some purposes and not for others. The larger the computer system, on the whole the greater the potential that its seizure will cause collateral damage to wholly innocent individuals and organizations; once a computer is seized the business that owned it is likely to come to a sharp halt, affecting employees, customers and creditors. In these circumstances there are no clear guidelines. Investigators then have to make a decision to leave the hardware *in situ*; hope to locate an employee of the raided firm who is technically competent but not under suspicion or other person, and supervise that person while copies of operating systems, logs, software and data are made. Section 19(4) of PACE permits a constable to "require any information which is contained in a computer and accessible from the premises [referred to in the warrant] to be produced in a form in which it can be taken away and in which it is visible and legible.″ The reference to "accessible from" seems to suggest that provided a warrant referred to a single relevant site, the whole, of a corporate network, wherever its components were located, would be included. In practice a selection may have to be made on grounds of cost and bulk. Investigators also need to acquire a detailed hardware and software inventory of the computer system, plus any reports prepared by EDP auditors and the like. If the computer system belongs to an international company, there may be different components in different jurisdictions and time-zones.

Once the raw evidence has been acquired, the problem is to show that it can be relied on. Again some of the tests developed in the Section 69 cases can be extended to other aspects of probative value. Thus, in the appeal in R. v. Cochrane which concerned print-out from an automated teller machine (ATM) connected to a complex banking/building society system, Waterhouse, J. observed: "It is with some surprise that we record that none of the witnesses who gave evidence in the Court below knew even the name of the town in which the mainframe computer was located." He concluded'

13.8.3 Evidence from the Internet:

Data recovered from mobile chat apps is critical to many forensic investigations. However, with thousands of mobile chat apps in use today and a steady stream of new apps emerging, identifying, recovering and analyzing mobile chat data is a significant challenge and has become a time consuming duty for forensic professionals.

There are two principal situations to be considered: where the offence is concentrated on an individual's use of the Internet and where a remote site holds evidence of an offence. Typical examples of the former include the downloading of paedophiliac material and unauthorized access; a great deal of evidence may exist on the accuser's own computer. Examples of the latter include: evidence of fraudulent promises to deliver goods, evidence of fraudulent offers to provide services, evidence of fraudulent or non-compliant investment offers, infringed copyright materials offered in the course of a business, holding or offering pornographic files and pictures, and incitements to racial hatred, terrorism and other offences, and conspiracies.

To understand where evidence of Internet-related offences may be located we need to recall how Internet connections are made and the forms they may take. Typically an individual uses his computer to connect to the Internet via an Internet Service Provider (ISP); home users dial in via a telephone network. There are thus four points at which evidence of various sorts may exist; on an individual's own computer, in his telephone bill, at the ISP and on remote sites. For law enforcement there is also the possibility of eavesdropping on Internet traffic in transit using a technique called "sniffing".

Considering, first, material held on a suspect's own computer, in addition to the material already referred to, PCs are likely hold the following Internet-specific logging files:

- E-mails sent and received are usually saved to hard-disk during routine use; however, most users regularly delete unwanted material to free up disk space;
- Newsgroups subscribed to are also usually saved to hard-disk during routine use; however again, most users regularly delete unwanted material to free up disk space;
- Internet Relay Chat (IRC) sessions are real-time discussions rather like CB radio; logging files which record what all participants have said are optional - There are also commercial and improved versions of IRC like Microsoft Net meeting and other products which provide Internet telephony and view phones; again logging may exist;
- Browser cache files are a specific sort of temporary file which is used to store data that the computer has recently used and may want again in the very near future. Although caching is used throughout computing, one of the most significant uses is within Internet browsers, the software used to visit sites on the World Wide Web. Here the cache stores copies of each web page as it is visited.

Users often need to revisit previously seen pages, particularly if they contain an index to other pages. The browser software can swiftly retrieve such a page from its cache rather than going back to the original source site (which would result in greater delay to the user and also

"This attachment of Love to God is indeed one that does not bind the soul but effectively breaks all its bondages."

add to the overall traffic on the Internet's main connections). In most browsers cache files are kept after individual sessions, often for weeks and months afterwards; some browsers and some specialist software can be used to view cache files and also associated "history" files which retain some date-and-time information. Thus it is possible to determine what the users of a specific computer have been viewing and, to a limited extent and after careful interpretation, when. There has been at least one attempt by prosecutors to assert that material saved in a web-browser cache but not otherwise intentionally retained constitutes "possession" for the purposes of Section 160, Criminal Justice Act, 1988.

It is sometimes possible to recover deleted logging files. However the completeness of any of these files, previously deleted or otherwise, and the extent to which date-and-time stamps are accurate is a matter that a person producing such forms of evidence must expect to be asked to demonstrate.

As regards telephone logs, private customers of ISPs usually dial-in via telephone — so, the logs provided by telephone companies showing numbers called, time and duration often give powerful corroboration to other types of evidence. Until relatively recently phone companies collected this type of information from specialist external devices attached to a subscriber's line: from an admissibility perspective it is possible to argue that the output of such call loggers or monitors is real evidence. More recently exhibits have been produced direct from the telephone company's regular billing computer. Although there are so far no recorded cases on the point, it could be argued that in these circumstances a proper Section 69, PACE certificate is needed as well as support to show that the exhibit is a "business etc document" for the purposes of Section 24 of the Criminal Justice Act, 1988. If law enforcement wish to capture data traffic on a telephone line between an ISP and its customer, the Interception of Communications Act, 1985 (ICOA) applies.

13.9 Are there any General Principles for Evaluating Computer Evidence?

Computer-derived evidence is not intrinsically different from other types of evidence produced in criminal proceedings. Rather the problems arise from the fragility and transience of may of the forms of computer evidence, the fact that provenance may be difficult to understand and the speed with which computer technology, and hence the evidence potentially available, changes.

There are few easy solutions. As we have seen, Waterhouse, J hoped for "a standard form of evidence" but English law is hostile to the idea of giving scientific or forensic evidence a juridical quality. In R. v. Dohenyf, DNA statistical evidence was produced in a rape and buggery case. The conviction was overturned on appeal on the basis that the expert had overstepped his role, restricting the role of the jury. A move to the US procedure of expecting Judges to act as the gatekeeper for novel scientific evidence, most recently considered in the 1993 US case of Daubert v. Merrell Dow, is not promising either. Even if the English Courts accepted the principle, it is doubtful whether some computer forensic evidence currently being tendered would meet the tests of (1) whether the theory or technique can be (and has been) tested; (2) the error rate associated with the method; (3) publication in a peer-reviewed journal; and (4) whether the technique has gained widespread acceptance. The Royal Commission on Criminal Justice chaired by Lord Runciman devoted Chapter 9 to a consideration of Forensic Science and Expert Evidence proposed *inter alia* the setting up a Forensic Science Council, but how well equipped would it be to assess skills in computer forensics? Similar concerns must apply to the notion of Court-appointed experts — how would they be selected? Many of these proposals would have the effect of denying the criminal justice system the benefits of the new techniques. And yet nearly all the arguments about incorporating forensic science within the adversarial procedure that arose around Runciman remain.

In effect, faced with new types of evidence the Courts have to fall back on general principles of evidence evaluation. Following are Miller's general tests for the reliability of an Exhibit. It should be possible to show that evidence is:

- Authentic - specifically linked to the circumstances and persons alleged — and produced by someone who can answer questions about such links;
- Accurate - free from any reasonable doubt about the quality of procedures used to collect the material, analyze the material if that is appropriate and necessary and finally to introduce it into Court and produced by someone who can explain what has been done. In the case of exhibits which themselves contain statements — a letter or other document, for example — "accuracy" must also encompass accuracy of content; and that normally requires the document's originator to make a Witness Statement and be available for cross-examination.
- Complete - tells within its own terms a complete story of particular set of circumstances or events.

In relation to more technical types of evidence — forensic evidence — we can expand on the range of attributes:

- There should be a clear chain of custody or continuity of evidence.
- A forensic method needs to be transparent, that is, freely testable by a third party expert. This creates difficulty if law enforcement think disclosure might result in the design of counter-measures which would prevent its future use; again the devisor of a forensic procedure may find it difficult to maintain commercial confidentiality.
- In the case of material derived from sources with which most people are not familiar quite extensive explanations may be needed.
- In the case of exhibits which themselves contain statements — a letter, database record or other document produced by a computer, for example — "accuracy" must encompass the accuracy of the process which produced the statement as well as accuracy of content; again normally that requires the document's originator to make a Witness Statement and be available for cross-examination.

In cases of "hacking" and other sophisticated computer crimes, there is an additional concern that the criminal modus operandi has computed the regular operation of a computer.

The more one looks at it, the clearer it becomes that we are not looking at one problem but several. Tempting as it initially might be to seek to draw up a simple list of types of computer evidence and "rate" them, certain problems become apparent quite soon; any such list ends up including "documents" or "statements" within the meanings of the various Civil and Criminal Evidence Acts (or that "common sense" first seems to suggest) but also types of evidence as produced by or recovered from computers. In the first category, we are identifying evidence by content and in the second by the form in which it has been held in or produced by a computer. Actually we need to do both. We need to know about the evidential weight of the content of a piece of computer-derived evidence, but we also need to know about the weight of the process by which it was produced. Process can, depending on the circumstances, contain several meanings as well — the quality of the original source, the quality of the internal computer manipulations, the strength of any control or audit mechanism which might reduce error or provide corroboration, the integrity of the way in which the exhibit — what the Court actually considers — has been derived, perhaps even the integrity of the way in which the exhibit has been handled by investigators.

13.10 Public Policy Issues:

Public policies regarding issues such as global hunger, conflict and peace, global health, migration, and global poverty all make an enormous impact on the lives of people living in poverty around the globe.

The proposed Code, unlike the current internal documents produced by law enforcement agencies, would be public and have been subjected to Parliamentary scrutiny. Among the advantages that might flow are it would provide guidance for a relatively new and rapidly developing source of evidence without the inflexibility of primary legislation. It would ensure fair, regular and consistent procedures and a vocabulary to describe them which would be recognized by the Courts. It could describe precautions for the safe acquisition and preservation of computers and hard-disks and forms of listing computer-derived materials in search registers. It would provide guidance for those issuing warrants. It would add to the existing framework for the maintenance of adequate safeguards and records. It would provide fair rules and procedures for the rapid seizure and return of computer hardware and data so that the activities and privacy of companies and individuals are not unduly penalised but without the need for constant recourse to the Police (Property) Act, 1897. It would give guidance for judges in assessing the process by which a computer-derived exhibit has arrived in Court and/or in assisting. It would provide greater fairness to the defence, including procedures for delivery of exhibits and access to specialist software necessary to review the validity of prosecution claims. It would lead to fewer "form" protests by the defence in Court or for irresponsible questioning of crown-experts as feared by the Law Commission in its Consultative Paper in 1995. It would reduce the costs of trials involving computer-related evidence by the avoidance of the delivery of unnecessarily bulky prosecution bundles of print-out and by allowing prosecution and defence experts access to electronic evidence which can then be analyzed with computers. It would provide a framework for specific training of law enforcement officers, leading to greater efficiencies and higher chances of success; while ensuring that fewer poor quality cases are presented to the Courts. Finally, it would provide the Legal Aid Board with guidance in assessing the requests for funding by defence interests.

अध्याय 14
Chapter 14
E-Mail Security

Notes :

14.1 Introduction:

In today’s electronic world, E-mail is critical to any business being competitive. In most cases it now forms the backbone of most organizations’ day-to-day activities, and its use will continue to grow.

E-mail addresses are extremely valuable in today’s economy. Referencing back to our quick calculation in the introduction, you can see that an E-mail address can be worth a lot of money to your business. Our identities, important accounts and vital information are attached to E-mail addresses. Chances are your financial institutions use your E-mail address as your username. Your social media accounts, like Facebook and Twitter, tie to your E-mail address. Your E-mail address is a unique identifier—but more importantly, it’s a communication mechanism. We use E-mail to transmit all kinds of important information, and we use E-mail more and more each day. Evil hackers want the E-mail accounts for various reasons.

The hacker wants your E-mail addresses to send you subscribers malicious stuff. Maybe your E-mail list has important users like Government Higher Officials. If they can trick your subscribers into clicking links and visiting bad sites, they can then gain access to machines they were targeting. Secure E-mail uses a set cryptographic tools to encapsulate a message into a specially formatted envelope. There are two environments being developed at the University of Aberdeen: one the RFC822 and SMTP mail system and the other, X.400. Two implementations are used: send mail, for SMTP, and Nexor's XT-PP for SMTP and X.400. The security aspects of these protocols and implementations will now be considered.

It has been stated by some that electronic mail is private and no - one has the right to read anyone elses messages. This may be the case if the rules of the institute have been thus formulated. It is normally the case that in, for example, the Unix world having super user access does not imply the right to read any messages although it does provide the mechanism. Care must be taken to maintain the privacy of mail. It should be an offence for an unauthorized person to read others mail. If care is not taken then encryption techniques will be employed end-to-end by users and then it is harder to prise out evidence from E-mail — a well-known problem with encryption. If evidence is forthcoming it must be handled properly so that it may be used in any resulting proceedings. This is an important area in itself together with the implications of the Police and Criminal Evidence Act for proper investigatory procedures.

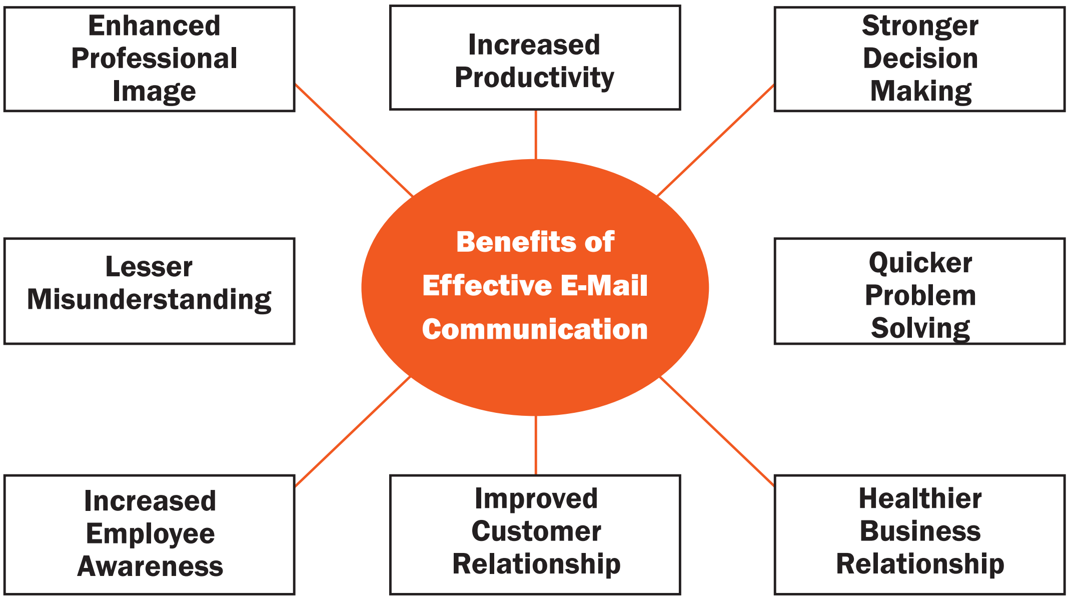

Enhanced Professional Image
Increased Productivity
Stronger Decision Making
Lesser Misunderstanding
Benefits of Effective E-Mail Communication
Quicker Problem Solving
Increased Employee Awareness
Improved Customer Relationship
Healthier Business Relationship

Fig. 14.1. E-mail Communication Benefits

Benefits of E-mail Communication:

The work in security for both SMTP/RFC822/MIME and X.400 are progressing very much in parallel with each other, addressing the same issues and proposing solutions which seem very similar. For the institute the risks are obvious with SMTP but as X.400 matures and is more widely used, the holes in it may appear. However, the X.400 framework seems better.

There are other E-mail systems based on Network Operating systems such as Novell, Windows for Workgroups. The underlying security of E-mail depends on the security features of these systems and the mail gateway require to transfer from the local to the SMTP or X.400 environment. The importance of E-mail continues to grow and the value of the information conveyed increases therefore the risk factor of any breach in security is more serious. Although no total solution can be offered for the 822/SMTP environment, some suggestions have been made to restrict the problem. It is the author's opinion that X.400 is basically a better vehicle but experience in the real world with X.400 is limited. As it is still a developing protocol it is hoped that it can still adapt — SMTP is fixed in tablets of stone. The legal aspects of mail have only been touched upon but experience indicates that this, and general nuisance mail, will involve more time than other violations. Nevertheless we continue to send and receive E-mail and trust the information conveyed by it with very little checking if any.

14.2 E-mail Content Filtering:

E-mail has become the leading form of communication making it essential for businesses to monitor the content of all messages entering and leaving their networks. Failure to do so can result in confidential, offensive, inappropriate or time-wasting messages compromising your E-mail communications.

Many firms now filter incoming E-mail messages (and sometimes outgoing messages) for dangerous or inappropriate content.

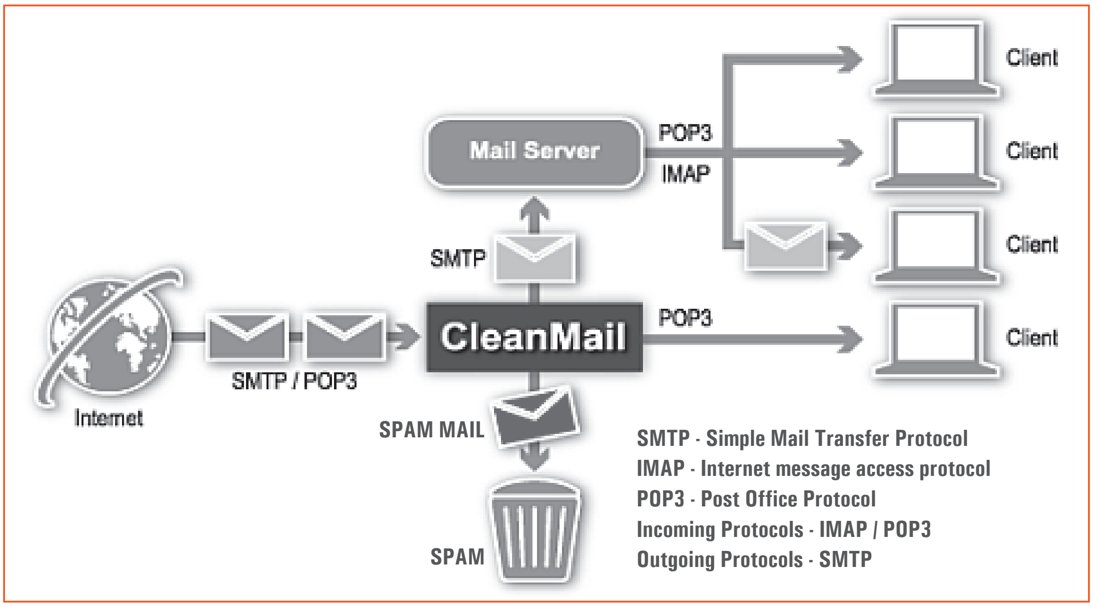

Client
Client
Client
Client
Mail Server
POP3
IMAP
SMTP
CleanMail
POP3
Internet
SMTP / POP3
SPAM MAIL
SPAM
SMTP - Simple Mail Transfer Protocol
IMAP - Internet message access protocol
POP3 - Post Office Protocol
Incoming Protocols - IMAP / POP3
Outgoing Protocols - SMTP

Fig. 14.2. Spam Filtering

14.3 Where to do E-mail Malware and Spam Filtering?

Malware is a software that is malicious in nature that can become installed on your computer, sometimes by no fault of your own. This malicious software can do anything from steal your passwords to websites, force you to purchase "antivirus" software (I'll get into that a bit more), or just cause your computer to be really slow because of how it runs in the background without your knowledge. One issue that companies face is where to do E-mail malware and spam filtering. Traditionally, this filtering was done on client PCs. Client filtering has several problems. Users often turn off their antivirus and anti-spam filters. They frequently fail to set up their systems properly for automatic downloading. They may even fail to maintain their subscription for receiving updates. If they do any of these things, they still will have antivirus and anti-spam software on their systems but no protection against new attacks.

In light of problems with client-based filtering, most companies now use filtering at the corporate E-mail server as the primary line of defence for E-mail this relegates client filtering to secondary importance as a defence-in-depth measure. E-mail administrators have the discipline and knowledge needed to manage E-mail filtering. In fact, E-mail administrators usually spend most of their time on antivirus filtering, spam filtering, and other security issues.

Due to the labour burdens of E-mail security, some companies are moving filtering entirely out of the firm, to E-mail managed service providers. Managed service providers reduce labour costs. They also have expertise in E-mail filtering.

Many companies do filtering at all three locations to increase defence in depth. At their corporate E-mail server, they may use a different filtering program than their managed service provider's use. Different antivirus and anti spam programs catch somewhat different threats.

14.4 E-mail Retention:

An E-mail retention policy is list of parameters created by an organization to determine what E-mail and instant messaging records need to be kept for compliance or other business reasons. The policy should also have a timetable for when records that have been retained can be moved to off-site storage archives or be destroyed.

Many mail servers store messages on their disk drives for some time, and then archive messages onto tape. The coordinated use of online storage and backup storage for messages is referred to as retention.

14.5 User Training:

E-mail can be a real Achilles heel, partly because it is so familiar that it is taken for granted. The fundamental security issues surrounding its use are all too often overlooked.

Much of this of course is down to lack of awareness and education. If an user or organization is not aware of the risks or exposures, appropriate controls and protection are hardly likely to be employed.

Although technology may help companies, the key to avoiding problems in the discovery process is to train users in what not to put into E-mail messages.

Users tend to think of E-mail messages as personal. However, the law does not view them that way. Discovery can dredge them up, they might be sent to the wrong party accidentally, and they can be forwarded to unintended parties. In addition, employers generally have the right to inspect E-mail messages and restrict messages to company business.

Employees must be taught never to put anything in a message that they would not want to see in court, printed in the newspapers, or read by their boss.

Users also need to be taught not to forward messages unless specifically authorized to do so. Once messages are forwarded, all control is lost. Even the list of original receivers can be damaging information.

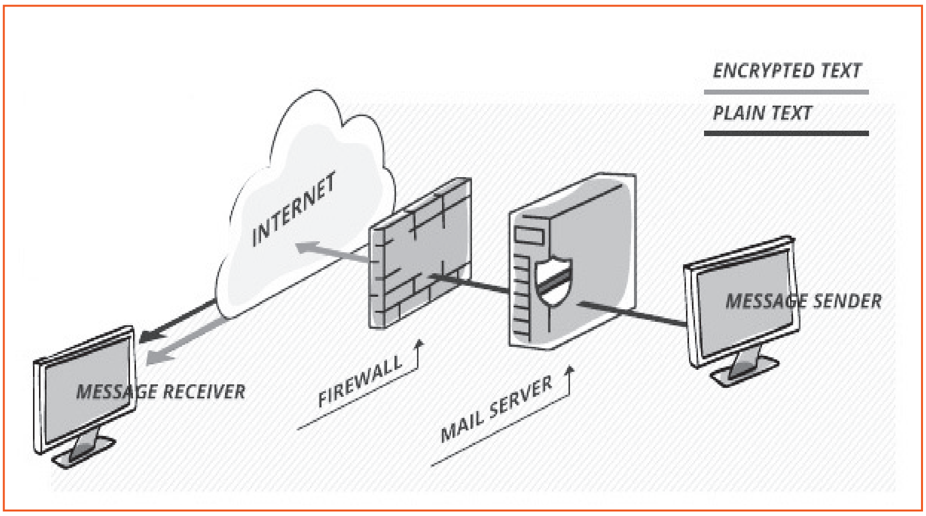


Fig. 14.3. E-Mail Encryption

Man acts only when he is sure of the justness of his action, as we threw the bomb in the Legislative Assembly.
- Shahid Bhaghat Singh

14.6 E-mail Encryption:

While en route from a sender to a recipient, an E-mail message may pass through several waypoints across the world before reaching its intended destination. Each of those waypoint networks pass along the message in-the-clear, meaning your E-mail, including attachments are available for anyone to read and steal, much like mailing a postcard. A single weak link along this path, a criminal port sniffing your network, and many other situations may compromise the confidential information of a message and can potentially result in leakage and exposure of sensitive information. The consequences of this happening can be detrimental, including brand erosion, loss of customer confidence, financial repercussions, legal penalties, regulatory violations and fines, and public embarrassment.

E-mail is a perfect candidate for cryptographic protection. However, relatively few corporations have their employees encrypt E-mail for confidentiality, authenticity, message integrity, or replay protection. One reason for this is the difficulty of using end-to-end encryption methods.

14.6.1 Voice over IP (VoIP) Security:
Sending Voice between Phones:

VoIP security issues are becoming increasingly serious because voice networks and services cannot be protected from recent intelligent attacks and fraud by traditional systems such as firewalls and NAT alone. After analyzing threats and recent patterns of attacks and fraud, consideration needs to be given to the redesign of secure VoIP architectures with advanced protocols and intelligent products, such as Session Border Controller (SBC). Another type of security issue is how to implement lawful interception within complicated service architectures according to government requirements.

The idea of VoIP is simple. Instead of calling someone else over the public switched telephone network, you call them over an IP internet.

When a person speaks, hardware or software called a codec in the VoIP phone converts the person’s voice into a stream of digital bytes. The VoIP phone then puts these bytes into packets and sends these packets to the other telephone.

Each packet carrying digital voice data has an IP header, followed by an User Datagram Protocol (UDP) header; an RTP header (discussed next), and a group of voice octets. These packets go directly between the two phones.

VoIP voice transmission uses UDP to carry the digital voice data. In VolP voice transmission, if a packet is lost, there is no time to wait for a retransmission to correct the loss. Consequently, there is no reason for TCP. The receiving codec merely inserts a packet’s worth of false sound based on preceding sound.

14.6.2 The Skype VoIP Service:

This guide will show you how to set up a service provider profile, change codec options (if necessary), and VoIP numbers for Skype VoIP service. When you start an account with Skype,

“Bless people when they revile you. Think how much good they are doing by helping to stamp out the false ego.”

they will provide you with account activation information. Use this information to activate Skype service, and to set up the service provider profile and VoIP numbers on your FortiVoice system. See the "VoIP Information" Section of the FortiVoice User Guide for instructions on how to connect your system to a network, set up IP addresses, configure the router, set up line hunt A groups, set up VoIP caller ID and reserve VoIP lines. The Skype public VoIP service currently offers free calling among Skype customers over the Internet and reduced-cost calling to and from Public Switched Telephone Network customers. Skype is extremely popular among consumers. However, many corporations ban Skype.

Skype uses proprietary software and protocols that have not been studied by security professionals. This causes security professionals to be concerned with the existence of vulnerabilities, backdoors, and other security threats.

Although Skype uses encryption for confidentiality, its method is unknown. Worse yet, Skype controls the encryption keys so that it can read traffic if it wants.

A particularly important point is that Skype does not provide adequate authentication. Although Skype authenticates users each time they enter the Skype network, initial registration is open and uncontrolled, so that usernames mean nothing from a security standpoint. An attacker can register other people's names and impersonate them.

Another problem is that Skype is a peer-to-peer (P2P) service that is almost impossible to control at firewalls because the Skype protocol is unknown and changes frequently to avoid analysis. Skype uses its structure to help users communicate through NAT firewalls. This is good for the user but bad for corporate security.

Nor does Skype's file transfer mechanism work with antivirus products at the time of this writing.

Overall, although most of these Skype concerns are theoretical, the fact that Skype cannot be well controlled by corporate security policies makes it unacceptable in many firms.

14.7 Data Security and Privacy:

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data. On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

Privacy in the information security context usually refers to the expectation and rights of individuals to privacy of their personal information and adequate, secure handling of this information by its users. Personal information here usually refers to information that directly identifies a human being, such as name and address, although the details may differ in different countries. In many countries, privacy of personal information is protected by laws that impose requirements on organizations processing personal data and set penalties for noncompliance. Since privacy is not only a basic human need but also a legally protected right in most countries, organizations should take necessary precautions to protect the confidentiality and integrity of personal information that they collect, store, and process. In particular, organizations' information security policies should define how personal information are to be collected and processed. Because of these requirements, although not in the C-I-A triad, privacy is also an inseparable part of information security and must be addressed in all information security policies as part of the information security requirements.

Information security is not only a technological challenge but a human challenge as well and needs human solutions first and foremost. For this reason, OECD member countries considered it necessary to develop Guidelines which would help to harmonize national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it. The key to maintaining security under these conditions is to reorient one's perspective on security. Protect the right things — privacy, for instance — and you can maintain reasonable security. Protect the wrong things, like secrecy, and you are doomed before you begin. The shelf life of a secret, especially in large organizations, is increasingly minuscule, and effectively limited only by the quickness with which modern technology can be leveraged to distribute such secrets beyond the set of people authorized to access those secrets.

The issue of data protection assumed great importance following the year 2000 and the development of internet-enabled services which, in turn, led to the boom in outsourcing of data processing, business process, call-centre services, accounting functions and other business operations first to local companies and then to countries such as India, China, Russia and the Philippines. As of 1995, the European Union had passed the Data Protection Directive, 95/46/ EC, which was soon implemented in European countries by national legislation such as the Data Protection Act of 1998 in the UK. In the absence of data protection legislation in India at that time and, indeed, even today there is no Data Protection Act in India, the question arose as to whether data transfers from the EU to India violated the European Data Protection Directive. Under the Data Protection Directive, all data transfers outside the EE A are *prima facie* illegal unless the recipient country ensures an 'adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data'.

Due to the lack of data protection legislation in India, in 2002, it was recommended that the model contractual clauses proposed by the EC Commission be adopted so as to create a

"Have Faith in Man, whether he appears to you to be a very learned one or a most ignorant one."

presumption of adequacy. However, in view of the parties' tendency to adopt different clauses, it was felt that additional measures were necessary. For example, the Working Document adopted on June 3, 2003, by the EU Data Protection Working Party recommended binding corporate codes for intra-corporate data transfers although the same were not legally binding. While such proposals were not forthcoming from the US, it was widely assumed that technical measures such as encryption were adopted by the US companies outsourcing to India to compensate for the lack of statutory data protection in India.

Over the decade which followed from the beginning of the outsourcing boom in 2002, India appeared to be on the verge of passing data protection legislation on several occasions. A Personal Data Protection Bill was introduced in Parliament in 2006, however, it was subsequently never passed. The Bill was not subsequently reintroduced in Parliament in later years. In fact, it was not until the 2009 amendments to the Information Technology Act 2000 that any statutory data protection provisions came into force.

This Chapter Examines the Following:

1) The data protection provisions introduced by the 2009 amendments to the IT Act and the Rules promulgated there under, including issues such as the handling of sensitive personal data and privacy rights at the workplace.

2) The Personal Data Protection Bill of 2006.

3) The development of Indian jurisprudence on privacy law towards protection of privacy rights in information.

4) An analysis of the key provisions of the EU Data Protection Directive in comparative analysis with the IT Act and Rules promulgated there under.

5) Privacy and the Telecommunications Sector – unsolicited commercial communications/ spamming under the Indian Telecoms Regulations in comparative analysis with the EU Privacy Directive (also known as the Cookies Directive).

6) Social networking and privacy issues.

अध्याय 15
Chapter 15

National Cyber Security Policy - 2013

Notes :

NATIONAL CYBER SECURITY POLICY-2013 (NCSP-2013) NOTIFICATION

Dated; 02 July. 2013

Subject: Notification on National Cyber Security Policy-2013 (NCSP-2013)

National Cyber Security Policy- 2013(NCSP-2013)

Preamble

1. Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e¬Learning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways), etc Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programms which have led to creation of large scale IT infrastructure with corporate / private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may

take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyberspace.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyberspace. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a National Cyber Security Policy, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non¬-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyberspace in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programms to enhance the security posture of country's cyberspace.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government.

II. Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. Objectives

1. To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

2. To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3. To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4. To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

5 To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

6 To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

7 To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

8 To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

9 To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10 To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to Cyber Crime or data theft.

11 To enable effective prevention, investigation and prosecution of Cyber Crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12 To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

13 To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14 To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

IV. Strategies

A. Creating a secure cyber ecosystem

1. To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

2. To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

3. To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

4. To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

5. To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.

6. To prevent occurrence and recurrence of cyber incidents by way of incentives for technology.

7. To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

8. To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

5) To encourage secure application / software development processes based on global best practices.

6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.

2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyberspace (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-ln) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-ln will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.

3) To operationalised 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.

4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

5) Toonduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.

2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

3) To engage information security professionals / organizations to assist e- Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

1. Todevelop a plan for protection of Critical Information Infrastructure and its

2. Integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

3. To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.

4. To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

5. To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.

6. To encourage and mandate as appropriate, the use of validated and certified IT products.

7. To mandate security audit of critical information infrastructure on a periodic basis.

8. To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

9. To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in Cyber Security

1) To undertake Research & Development programs for addressing all aspects of Development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

3) To facilitate transition, diffusion and commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.

4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyberspace.

5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

I. Reducing supply chain risks

1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.

3) To create awareness of the threats, vulnerabilities and consequences of breach of Security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

J. Human Resource Development

1) To foster education and training programs both in formal and informal sectors to Support the Nation's cyber security needs and build capacity.

2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

3) To establish cyber security concept labs for awareness and skill development in key areas.

4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

1) To promote and launch a comprehensive national awareness program on security of cyberspace.

2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.

3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

2) To create models for collaborations and engagement with all relevant stakeholders.

3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.

2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.

3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

N. Prioritized approach for implementation

1) To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

(J. Satyanarayana)
Secretary, DeitY
Tel: 24364041

New Delhi, Dated: 02 July 2013

Copy to:

1. All Concerned Ministries/ Departments of Government of India Cabinet Secretariat
2. PMO
3. Planning Commission
4. Comptroller and Auditor General of India
5. JS & FA. Department of Electronics and Information Technology
6. Internal Distribution

(J. Satyanarayana)
Secretary, DeitY
Tel: 24364041

References

1. Cyber Crime in India By Dr. M. Dasgupta (Eastern Law House Publications)
2. Investigation of Cyber Crimes By Alex Samuel & A.K. Upadhyay (Dwivedi & Company)
3. Cyber Law By Aparna Viswanathan (Lexis Nexis Butterworths Wadhwa)
4. Corporate Computer and Network Security (2nd Edition) By Raymond R. Panko
5. "Cyber Crimes, Law Enforcement, Security & Surveillance in the Information Age." By D. Thomas & B.D. Loader
6. Fighting Computer Crime, (Wiley Computer Publishing) By D.B. Parker
7. Cyber Shock By W. Schwartau (Thunder's Mouth Press)
8. Introduction to Computer Law By David Bainbridge(4th edition)
9. International Computer Crimes Conference, "Internet as the Scene of Crime" by James K. Robinson
10. "Emerging Challenge: Security and Safety in Cyberspace," by Hundley, R. & Anderson, R
11. "Far right extremities on the internet" By Michael Whine
12. "The Policies of Hacking" By Douglas Thomas
13. "Computer Forensics" By John R. Vacca

Glossary

Access Control

Access Control ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL)

A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control Service

A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

Access Management Access

Management is the maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation.

Access Matrix

An Access Matrix uses rows to represent subjects and columns to represent objects with privileges listed in each cell.

Account Harvesting

Account Harvesting is the process of collecting all the legitimate account names on a system.

ACK Piggybacking

ACK piggybacking is the practice of sending an ACK inside another packet going to the same destination.

Active Content

Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS)

Activity Monitors

Activity monitors aim to prevent virus infection by monitoring for malicious activity on a system, and blocking that activity when possible.

Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Advanced Encryption Standard (AES)

An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

Algorithm

A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer.

Applet

Java programs; an application program that uses the client's web browser to provide a user interface.

Arpanet

Advanced Research Projects Agency Network, a pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.

Asymmetric Cryptography

Public-key cryptography; A modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

Asymmetric Warfare

Asymmetric warfare is the fact that a small investment, properly leveraged, can yield incredible results.

Auditing

Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

Authentication

Authentication is the process of confirming the correctness of the claimed identity.

Authenticity

Authenticity is the validity and conformance of the original information.

Authorization

Authorization is the approval, permission, or empowerment for someone or something to do something.

Autonomous System

One network or series of networks that are all under one administrative control. An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Availability

Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

Backdoor

A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.

Bandwidth

Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

Banner

A banner is the information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use.

Basic Authentication

Basic Authentication is the simplest web-based authentication scheme that works by sending the username and password with each request.

Bastion Host

A bastion host has been hardened in anticipation of vulnerabilities that have not been discovered yet.

BIND

BIND stands for Berkeley Internet Name Domain and is an implementation of DNS. DNS is used for domain name to IP address resolution.

Biometrics

Biometrics use physical characteristics of the users to determine access.

Bit

The smallest unit of information storage; a contraction of the term "binary digit;" one of two symbolsÑ"0" (zero) and "1" (one) - that are used to represent binary numbers.

Block Cipher

A block cipher encrypts one block of data at a time.

Boot Record Infector

A boot record infector is a piece of malware that inserts malicious code into the boot sector of a disk.

Border Gateway Protocol (BGP)

An inter-autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

Botnet

A botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.

BOTS

Programs that are installed covertly on a user's system which allows the attacker to remotely control the targeted computer through a communication channel such as Internet relay chat(IRC), peer-to-peer (P2P), or HTTP.

Bridge

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).

Broadcast

To simultaneously send the same message to multiple recipients. One host to all hosts on network.

Broadcast Address

An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

Browser

A client computer program that can retrieve and display information from servers on the World Wide Web.

Brute Force

A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

Buffer Overflow

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Business Continuity Plan (BCP)

A Business Continuity Plan is the plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Business Impact Analysis (BIA)

A Business Impact Analysis determines what levels of impact to a system are tolerable.

Byte

A fundamental unit of computer storage; the smallest addressable unit in a computer's architecture. Usually holds one character of information and usually means eight bits.

Cache

Pronounced cash, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

Cache Cramming

Cache Cramming is the technique of tricking a browser to run cached Java code from the local disk, instead of the internet zone, so it runs with less restrictive permissions.

Cache Poisoning

Malicious or misleading data from a remote name server is saved [cached] by another name server. Typically used with DNS cache poisoning attacks.

Call Admission Control (CAC)

The inspection and control all inbound and outbound voice network activity by a voice firewall based on user-defined policies.

Carnivore Software

Software that uses packet sniffing at the ISP level to monitor data flow through ISPs. Carnivore is designed to monitor email and electronic communications. It is known as a customized packet sniffer which can be used to monitor all of the internet traffic of a particular user.

Cell

A cell is a unit of data transmitted over an ATM network.

Certificate-Based Authentication

Certificate-Based Authentication is the use of SSL and certificates to authenticate and encrypt HTTP traffic.

CGI

Common Gateway Interface. This mechanism is used by HTTP servers (web servers) to pass parameters to executable scripts in order to generate responses dynamically.

Chain of Custody

Chain of Custody is the important application of the Federal rules of evidence and its handling.

Challenge-Handshake Authentication Protocol (CHAP)

The Challenge-Handshake Authentication Protocol uses a challenge/response authentication mechanism where the response varies every challenge to prevent replay attacks.

Checksum

A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

Cipher

A cryptographic algorithm for encryption and decryption.

Ciphertext

Ciphertext is the encrypted form of the message being sent.

Circuit Switched Network

A circuit switched network is where a single continuous physical circuit connected two endpoints where the route was immutable once set up.

Client

A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

Cloud Bursting

A process where a service provided by a private cloud can automatically access and use resources from a public cloud when it needs to ramp up and handle peak demand.

Computer-related forgery

Computer-related forgery involves the unauthorized creating or altering or manipulation of stored data so that they acquire a different evidentiary value in the course of legal transactions which relies on the authentically of information contained in the data.

Computer-related fraud

The causing of loss of property to another person by manipulating or altering, deleting any computer data, with fraudulent or dishonest intention to gain economic benefit without right, is considered as computer-related fraud.

Collision

A collision occurs when multiple systems transmit simultaneously on the same wire.

Competitive Intelligence

Competitive Intelligence is espionage using legal, or at least not obviously illegal, means.

Computer Emergency Response Team (CERT)

An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

Computer Network

A collection of host computers together with the sub-network or inter-network through which they can exchange data.

Confidentiality

Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

Configuration Management

Establish a known baseline condition and manage it.

Cookie

Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections.

Corruption

A threat action that undesirably alters system operation by adversely modifying system functions or data.

Cost Benefit Analysis

A cost benefit analysis compares the cost of implementing countermeasures with the value of the reduced risk.

Counter Measure

Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ counter measures to prevent intruders form gaining further access to a computer network. Other counter measures are patches, access control lists and malware filters.

Covert Channels

Covert Channels are the means by which information can be communicated between two parties in a covert fashion using normal system operations. For example by changing the amount of hard drive space that is available on a file server can be used to communicate information.

Cron

Cron is a Unix application that runs jobs for users and administrators at scheduled times of the day.

Crossover Cable

A crossover cable reverses the pairs of cables at the other end and can be used to connect devices directly together.

Cryptanalysis

The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.

Cryptographic Algorithm or Hash

An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.

Cut-Through

Cut-Through is a method of switching where only the header of a packet is read before it is forwarded to its destination.

Cyclic Redundancy Check (CRC)

Sometimes called "cyclic redundancy code." A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

Daemon

A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term, though many other operating systems provide support for daemons, though they're sometimes called other names. Windows, for example, refers to daemons and System Agents and services.

Data Aggregation

Data Aggregation is the ability to get a more complete picture of the information by analyzing several different types of records at once.

Data Custodian

A Data Custodian is the entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.

Data Encryption Standard (DES)

A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Data Interference

Data interference means damaging, deletion, deterioration, alteration or suppression of computer data, intentionally and without a right to do so and input of malicious codes, such as viruses and Trojan horses.

Data Mining

Data Mining is a technique used to analyze existing information, usually with the intention of pursuing new avenues to pursue business.

Data Owner

A Data Owner is the entity having responsibility and authority for the data.

Data Preservation

Data preservation means keeping data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate.

Data Retention

Data retention means the accumulation of data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate.

Data Warehousing

Data Warehousing is the consolidation of several previously independent databases into one location.

Datagram

Datagram's or packets are the message units that the Internet Protocol deals with and that the Internet transports. A datagram or packet needs to be self-contained without reliance on earlier exchanges because there is no connection of fixed duration between the two communicating points as there is, for example, in most voice telephone conversations. (This kind of protocol is referred to as connectionless.)

Day Zero

The “Day Zero” or “Zero Day” is the day a new vulnerability is made known. In some cases, a “zero day” exploit is referred to an exploit for which no patch is available yet. (“day one”-> day at which the patch is made available).

Decapsulation

Decapsulation is the process of stripping off one layer’s headers and passing the rest of the packet up to the next higher layer on the protocol stack.

Decryption

Decryption is the process of transforming an encrypted message into its original plaintext.

Deep Packet Inspection

Interception of online data from emails, internet phone calls, as well as images on social networking sites, such as Facebook and Twitter. Every digitized packet of online data is intercepted, de-constructed, examined for keywords and then reconstructed within a few milliseconds.

Defacement

Defacement is the method of modifying the content of a website in such a way that it becomes “vandalized” or embarrassing to the website owner.

Defence In-Depth

Defence In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.

Denial of Service

The prevention of authorized access to a system resource or the delaying of system operations and functions.

Dictionary Attack

An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

Diffie-Hellman

A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

Digest Authentication

Digest Authentication allows a web client to compute MD5 hashes of the password to prove it has the password.

Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital Envelope

A digital envelope is an encrypted message with the encrypted session key.

Digital Signature

A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

Digital Signature Algorithm (DSA)

An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Digital Signature Standard (DSS)

The US Government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

Disassembly

The process of taking a binary program and deriving the source code from it.

Disaster Recovery Plan (DRP)

A Disaster Recovery Plan is the process of recovery of IT systems in the event of a disruption or disaster.

Discretionary Access Control (DAC)

Discretionary Access Control consists of something the user can manage, such as a document password.

Disruption

A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Distance Vector

Distance vectors measure the cost of routes to determine the best route to all known networks.

Distributed Scans

Distributed Scans are scans that use multiple source addresses to gather information.

Domain

A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

Domain Hijacking

Domain hijacking is an attack by which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name

A domain name locates an organization or other entity on the Internet. For example, the domain name "www.nationalcybersafety.com" locates an Internet address for "nationalcybersafety.com" and a particular host server named "www". The "com" part of the domain name reflects the purpose of the organization or entity (in this example, "commerce") and is called the top-level domain name.

Domain Name System (DNS)

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Due Care

Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

Due Diligence

Due diligence is the requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

DumpSec

DumpSec is a security tool that dumps a variety of information about a system's users, file system, registry, permissions, password policy, and services.

Dumpster Diving

Dumpster Diving is obtaining passwords and corporate directories by searching through discarded media.

Dynamic Link Library

A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

Dynamic Routing Protocol

Allows network devices to learn routes. Ex. RIP, EIGRP Dynamic routing occurs when routers talk to adjacent routers, informing each other of what networks each router is currently connected to. The routers must communicate using a routing protocol, of which there are many to choose from. The process on the router that is running the routing protocol, communicating with its neighbour routers, is usually called a routing daemon. The routing daemon updates the kernel's routing table with information it receives from neighbour routers.

Eavesdropping

Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network.

Echo Reply

An echo reply is the response a machine that has received an echo request sends over ICMP.

Echo Request

An echo request is an ICMP message sent to a machine to determine if it is online and how long traffic takes to get to it.

Egress Filtering

Filtering outbound traffic.

Emanations Analysis

Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Encapsulation

The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

Encryption

Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Ephemeral Port

Also called a transient port or a temporary port. Usually is on the client side. It is set up when a client application wants to connect to a server and is destroyed when the client application terminates. It has a number chosen at random that is greater than 1023.

Escrow Passwords

Escrow Passwords are passwords that are written down and stored in a secure location (like a safe) that are used by emergency personnel when privileged personnel are unavailable.

Ethernet

The most widely-installed LAN technology. Specified in a standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Devices are connected to the cable and compete for access using a CSMA/CD protocol.

Event

An event is an observable occurrence in a system or network.

Exponential Backoff Algorithm

An exponential backoff algorithm is used to adjust TCP timeout values on the fly so that network devices don't continue to timeout sending data over saturated links.

Exposure

A threat action whereby sensitive data is directly released to an unauthorized entity.

Extended ACLs (Cisco)

Extended ACLs are a more powerful form of Standard ACLs on Cisco routers. They can make filtering decisions based on IP addresses (source or destination), Ports (source or destination), protocols, and whether a session is established.

Extensible Authentication Protocol (EAP)

A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences.

Exterior Gateway Protocol (EGP)

A protocol which distributes routing information to the routers which connect autonomous systems.

False Rejects

False Rejects are when an authentication system fails to recognize a valid user.

Fast File System

The first major revision to the Unix file system, providing faster read access and faster (delayed, asynchronous) write access through a disk cache and better file system layout on disk. It uses inodes (pointers) and data blocks.

Fast Flux

Protection method used by botnets consisting of a continuous and fast change of the DNS records for a domain name through different IP addresses.

Fault Line Attacks

Fault Line Attacks use weaknesses between interfaces of systems to exploit gaps in coverage.

File Transfer Protocol (FTP)

A TCP/IP protocol specifying the transfer of text or binary files across the network.

Filter

A filter is used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

Filtering Router

An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network.

A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.

Fingerprinting

Sending strange packets to a system in order to gauge how it responds to determine the operating system.

Firewall

A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

Flooding

An attack that attempts to cause a failure in (especially, in the security of) a computer system or other data processing entity by providing more input than the entity can process properly.

Forest

A forest is a set of Active Directory domains that replicate their databases with each other.

Fork Bomb

A Fork Bomb works by using the fork() call to create a new process which is a copy of the original. By doing this repeatedly, all available processes on the machine can be taken up.

Form-Based Authentication

Form-Based Authentication uses forms on a webpage to ask a user to input username and password information.

Forward Lookup

Forward lookup uses an Internet domain name to find an IP address.

Forward Proxy

Forward Proxies are designed to be the server through which all requests are made.

Fragment Offset

The fragment offset field tells the sender where a particular fragment falls in relation to other fragments in the original larger packet.

Fragmentation

The process of storing a data file in several "chunks" or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

Frames

Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that "frame" the data. (Some control frames contain no data.)

"The will is not free - it is a phenomenon bound by cause and effect - but there is something behind the will which is free."

Framing

An act of fraudulent display of contents of one website within another person's website with the purpose of making the user believe that he is actually viewing the former's website. Third party content is used intentionally within the frames of the website.

Full Duplex

A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.

Fully-Qualified Domain Name

A Fully-Qualified Domain Name is a server name with a hostname followed by the full domain name.

Fuzzing

The use of special regression testing tools to generate out-of-spec input for an application in order to find security vulnerabilities.

Gateway

A network point that acts as an entrance to another network.

Gethostbyaddr

The gethostbyaddr DNS query is when the address of a machine is known and the name is needed.

Gethostbyname

The gethostbyname DNS quest is when the name of a machine is known and the address is needed.

GNU

GNU is a Unix-like operating system that comes with source code that can be copied, modified, and redistributed. The GNU project was started I n 1983 by Richard Stallman and others, who formed the Free Software Foundation.

Gnutella

An Internet file sharing utility. Gnutella acts as a server for sharing files while simultaneously acting as a client that searches for and downloads files from other users.

Hacking

Gaining of unauthorized access to the data stored in computer systems. Hacking is an intentional act of breaking into a computer system with the objective of stealing data that can be used for purposes of identity theft or other fraud.

Hactivism

Hactivism is a term which combines the concepts of 'hacking' and 'activism' which means the hacking into the computer system of another for a social or a political purpose.

Hardening

Hardening is the process of identifying and fixing vulnerabilities on a system.

Hash Function

An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

Hash Functions

(cryptographic) hash functions are used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHAL.

Header

A header is the extra information in a packet that is needed for the protocol stack to process the packet.

Hijack Attack

A form of active wiretapping in which the attacker seizes control of a previously established communication association.

Honey Client

see Honeymonkey.

Honey pot

Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Honeymonkey

Automated system simulating a user browsing websites. The system is typically configured to detect web sites which exploit vulnerabilities in the browser. Also known as Honey Client.

Hops

A hop is each exchange with a gateway a packet takes on its way to the destination.

Host

Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

HTTP Proxy

An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

HTTPS

When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.

Hub

A hub is a network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub.

Hybrid Attack

A Hybrid Attack builds on the dictionary attack method by adding numerals and symbols to dictionary words.

Hybrid Cloud

A hybrid cloud is a composition of two or more clouds (private or public) that remain separate cloud entities but share certain technology which permits interoperability.

Hybrid Encryption

An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

Hyperlink

In hypertext or hypermedia, an information object (such as a word, a phrase, or an image; usually highlighted by colour or underscoring) that points (indicates how to connect) to related information that is located elsewhere and can be retrieved by activating the link.

Hypertext Mark-up Language (HTML)

The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

Hypertext Transfer Protocol (HTTP)

The protocol in the Internet Protocol (IP) family used to transport hypertext documents across an internet.

Identity

Identity is whom someone or what something is, for example, the name by which something is known.

Incident

An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event.

Incident Handling

Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Incremental Backups

Incremental backups only backup the files that have been modified since the last backup. If dump levels are used, incremental backups only backup files changed since last backup of a lower dump level.

Inetd (xinetd)

Inetd (or Internet Daemon) is an application that controls smaller internet services like telnet, ftp, and POP.

Inference Attack

Inference Attacks rely on the user to make logical connections between seemingly unrelated pieces of information.

Information Warfare

Information Warfare is the competition between offensive and defensive players over information resources.

Ingress Filtering

Ingress Filtering is filtering inbound traffic.

Input Validation Attacks

Input Validations Attacks are where an attacker intentionally sends unusual input in the hopes of confusing an application.

Integrity

Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

Integrity Star Property

In Integrity Star Property a user cannot read data of a lower integrity level then their own.

Internet

A term to describe connecting multiple separate networks together.

Internet Control Message Protocol (ICMP)

An Internet Standard protocol that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.

Internet Engineering Task Force (IETF)

The body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership.

Internet Message Access Protocol (IMAP)

A protocol that defines how a client should fetch mail from and return mail to a mail server. IMAP is intended as a replacement for or extension to the Post Office Protocol (POP). It is defined in RFC 1203 (v3) and RFC 2060 (v4).

Internet Protocol (IP)

The method or protocol by which data is sent from one computer to another on the Internet.

Internet Protocol Security (IPsec)

A developing standard for security at the network or packet processing layer of network communication.

Internet Standard

A specification, approved by the IESG and published as an RFC, that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.

Interrupt

An Interrupt is a signal that informs the OS that something has occurred.

Intranet

A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

Intrusion Detection

A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Address

A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP Flood

A denial of service attack that sends a host more echo request ("ping") packets than the protocol implementation can handle.

IP Forwarding

IP forwarding is an Operating System option that allows a host to act as a router. A system that has more than 1 network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP Spoofing

The technique of supplying a false IP address.

ISO

International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

Issue-Specific Policy

An Issue-Specific Policy is intended to address specific needs within an organization, such as a password policy.

ITU-T

International Telecommunications Union, Telecommunication Standardization Sector (formerly "CCITT"), a United Nations treaty organization that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations."

Jitter

Jitter or Noise is the modification of fields in a database while preserving the aggregate characteristics of that make the database useful in the first place.

Jump Bag

A Jump Bag is a container that has all the items necessary to respond to an incident inside to help mitigate the effects of delayed reactions.

Kerberos

A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.

Kernel

The essential centre of a computer operating system, the core that provides basic services for all other parts of the operating system. A synonym is nucleus. A kernel can be contrasted with a shell, the outermost part of an operating system that interacts with user commands. Kernel and shell are terms used more frequently in Unix and some other operating systems than in IBM mainframe systems.

Key Loggers

A software program or a device designed to secretly monitor and log all keystrokes. Key logging devices are small devices that can be fixed to the keyboard, or placed within a cable or the computer itself. Key logging software is made up of programs dedicated to tracking and logging keystrokes.

Lattice Techniques

Lattice Techniques use security designations to determine access to information.

Layer 2 Forwarding Protocol (L2F)

An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user.

Layer 2 Tunneling Protocol (L2TP)

An extension of the Point-to-Point Tunnelling Protocol used by an Internet service provider to enable the operation of a virtual private network over the Internet.

Lawful Interception

Legally sanctioned official access to private communications such as telephone calls and email messages

Location Data

Data which provide the geographic position of the mobile phone user.

Least Privilege

Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

Legion

Software to detect unprotected shares.

Lightweight Directory Access Protocol (LDAP)

A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

Link State

With link state, routes maintain information about all routers and router-to-router links within a geographic area, and create a table of best routes with that information.

Linking

Linking occurs where the URL, that is, the website address provided connects to a specific page on a website rather than the home page.

List Based Access Control

List Based Access Control associates a list of users and their privileges with each object.

Loadable Kernel Modules (LKM)

Loadable Kernel Modules allow for the adding of additional functionality directly into the kernel while the system is running.

Log Clipping

Log clipping is the selective removal of log entries from a system log to hide a compromise.

Logic bombs

Logic bombs are programs or snippets of code that execute when a certain predefined event occurs. Logic bombs may also be set to go off on a certain date or when a specified set of circumstances occurs.

Logic Gate

A logic gate is an elementary building block of a digital circuit. Most logic gates have two inputs and one output. As digital circuits can only understand binary, inputs and outputs can assume only one of two states, 0 or 1.

Loopback Address

The loopback address (127.0.0.1) is a pseudo IP address that always refer back to the local host and are never sent out onto a network.

MAC Address

A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

Malicious Code

Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

Malware

A generic term for a number of different types of malicious code.

Mandatory Access Control (MAC)

Mandatory Access Control controls is where the system controls access to resources based on classification levels assigned to both the objects and the users. These controls cannot be changed by anyone.

Masquerade Attack

A type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity.

MD5

A one way cryptographic hash function. Also see "hash functions" and "shAL"

Measures of Effectiveness (MOE)

Measures of Effectiveness is a probability model based on engineering concepts that allows one to approximate the impact a give action will have on an environment. In Information warfare it is the ability to attack or defend within an Internet environment.

Meta Tags

A meta tag is an encoded statement in the Hypertext Mark-up Language (HTML) that provides information regarding some of the content of a webpage. The meta tag is placed near the top of the HTML in a web page as a part of the heading. Based on the information fed into a meta tag by the net surfer, search engines index the pages which could be of interest to an internet user.

Monoculture

Monoculture is the case where a large number of users run the same software, and are vulnerable to the same attacks.

Morris Worm

A worm program written by Robert T. Morris, Jr. that flooded the ARPANET in November, 1988, causing problems for thousands of hosts.

Multi-Cast

Broadcasting from one host to a given set of hosts.

Multi-Homed

You are "multi-homed" if your network is directly connected to two or more ISP's.

Multiplexing

To combine multiple signals from possibly disparate sources, in order to transmit them over a single path.

NAT

Network Address Translation. It is used to share one or a small number of publicly routable IP addresses among a larger number of hosts. The hosts are assigned private IP addresses, which are then "translated" into one of the publicly routed IP addresses. Typically home or small business networks use NAT to share a single DLS or Cable modem IP address. However, in some cases NAT is used for servers as an additional layer of protection.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology, a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

Natural Disaster

Any "act of God" (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.

Netmask

32-bit number indicating the range of IP addresses residing on a single IP network/subnet/supernet. This specification displays network masks as hexadecimal numbers. For example, the network mask for a class C IP network is displayed as 0xffffff00. Such a mask is often displayed elsewhere in the literature as 255.255.255.0.

Network Address Translation

The translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

Network Mapping

To compile an electronic inventory of the systems and the services on your network.

Network Taps

Network taps are hardware devices that hook directly onto the network cable and send a copy of the traffic that passes through it to one or more other networked devices.

Network-Based IDS

A network-based IDS system monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments, and traffic on other means of communication (like phone lines) can't be monitored. Network-based IDS involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment it's attached to. Packets are considered to be of interest if they match a signature. Network-based intrusion detection passively monitors network activity for indications of attacks. Network monitoring offers several advantages over traditional host-based intrusion detection systems. Because many intrusions occur over networks at some point, and because networks are increasingly becoming the targets of attack, these techniques are an excellent method of detecting many attacks which may be missed by host-based intrusion detection mechanisms.

Non-Repudiation

Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

Null Session

Known as Anonymous Logon, it is a way of letting an anonymous user retrieve information such as user names and shares over the network or connect without authentication. It is used by applications such as explorer.exe to enumerate shares on remote servers.

Octet

A sequence of eight bits. An octet is an eight-bit byte.

One-Way Encryption

Irreversible transformation of plaintext to cipher text, such that the plaintext cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known.

One-Way Function

A (mathematical) function, f, which is easy to compute the output based on a given input. However given only the output value it is impossible (except for a brute force attack) to figure out what the input value is.

Open Shortest Path First (OSPF)

Open Shortest Path First is a link state routing algorithm used in interior gateway routing. Routers maintain a database of all routers in the autonomous system with links between the routers, link costs, and link states (up and down).

OSI

OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. Its

"The earth is enjoyed by heroes" – this is the unfailing truth. Be a hero. Always say, "I have no fear."

purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the OSI model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

Overload

Hindrance of system operation by placing excess burden on the performance capabilities of a system component.

Packet

A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Packet Switched Network

A packet switched network is where individual packets each follow their own paths through the network from one endpoint to another.

Partitions

Major divisions of the total physical hard disk space.

Password Authentication Protocol (PAP)

Password Authentication Protocol is a simple, weak authentication mechanism where a user enters the password and it is then sent across the network, usually in the clear.

Password Cracking

Password cracking is the process of attempting to guess passwords, given the password file information.

Password Sniffing

Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Patch

A patch is a small update released by a software manufacturer to fix bugs in existing programs.

Patching

Patching is the process of updating software to a different version.

Payload

Payload is the actual application data a packet contains.

Penetration

Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Penetration Testing

Penetration testing is used to test the external perimeter security of a network or facility.

Permutation

Permutation keeps the same letters but changes the position within a text to scramble the message.

Personal Data

The information or data which relate to a living individual who can be identified from that information or data, whether collected by any Government or any private organization or agency.

Personal Firewalls

Personal firewalls are those firewalls that are installed and run on individual PCs.

Pharming

This is a more sophisticated form of MITM attack. A user's session is redirected to a masquerading website. This can be achieved by corrupting a DNS server on the Internet and pointing a URL to the masquerading website's IP. Almost all users use a URL like www.worldbank.com instead of the real IP (192.86.99.140) of the website. Changing the pointers on a DNS server, the URL can be redirected to send traffic to the IP of the pseudo website. At the pseudo website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real www.worldbank.com site and conduct transactions using the credentials of a valid user on that website.

Phishing

The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

Phreaking

The word 'phreaking' is a combination of the two words 'phone' and 'freak'. Phreaking refers to people who tamper with systems of telecommunications such as the public telephone networks and various phone system audio frequencies.

Ping of Death

An attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

Ping Scan

A ping scan looks for machines that are responding to ICMP Echo Requests.

Ping Sweep

An attack that sends ICMP echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

Plaintext

Ordinary readable text before being encrypted into ciphertext or after being decrypted.

Point-to-Point Protocol (PPP)

A protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. It packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

Point-to-Point Tunneling Protocol (PPTP)

A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet.

Poison Reverse

Split horizon with poisoned reverse (more simply, poison reverse) does include such routes in updates, but sets their metrics to infinity. In effect, advertising the fact that there routes are not reachable.

Polyinstantiation

Polyinstantiation is the ability of a database to maintain multiple records with the same key. It is used to prevent inference attacks.

Polymorphism

Polymorphism is the process by which malicious software changes its underlying code to avoid detection.

Port

A port is nothing more than an integer that uniquely identifies an endpoint of a communication stream. Only one process per machine can listen on the same port number.

Possession

Possession is the holding, control, and ability to use information.

Post Office Protocol, Version 3 (POP3)

An Internet Standard protocol by which a client workstation can dynamically access a mailbox on a server host to retrieve mail messages that the server has received and is holding for the client.

Practical Extraction and Reporting Language (Perl)

A script programming language that is similar in syntax to the C language and that includes a number of popular Unix facilities such as sed, awk, and tr.

Pretty Good Privacy (PGP)TM

Trademark of Network Associates, Inc., referring to a computer program (and related protocols) that uses cryptography to provide data security for electronic mail and other applications on the Internet.

Private Addressing

IANA has set aside three address ranges for use by private or non-Internet connected networks. This is referred to as Private Address Space and is defined in RFC 1918. The reserved address blocks are: 10.0.0.0 to 10.255.255.255 (10/8 prefix) 172.16.0.0 to 172.31.255.255 (172.16/12 prefix) 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

Private Cloud

A private cloud (also called internal cloud) is one in which the computing environment is operated exclusively for a particular company or organization. The private cloud providers services to a limited number of users behind a firewall.

Processing

Processing means obtaining, recording or holding the personal data or information of an individual and carrying out any operation on the information including alteration, disclosure, transmission, dissemination and destruction.

Program Infector

A program infector is a piece of malware that attaches itself to existing program files.

Program Policy

A program policy is a high-level policy that sets the overall tone of an organization's security approach.

Promiscuous Mode

When a machine reads all packets off the network, regardless of who they are addressed to. This is used by network administrators to diagnose network problems, but also by unsavory characters who are trying to eavesdrop on network traffic (which might contain passwords or other information).

Proprietary Information

Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

Protocol

A formal specification for communicating; an IP address the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection.

Protocol Stacks (OSI)

A set of network protocol layers that work together.

Proxy Server

A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Public Cloud

A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the internet.

Public Key

The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

Public Key Encryption

The popular synonym for “asymmetric cryptography”.

Public Key Infrastructure (PKI)

A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

Public-Key Forward Secrecy (PFS)

For a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

QAZ

A network worm.

Race Condition

A race condition exploits the small window of time between a security control being applied and when the service is used.

Radiation Monitoring

Radiation monitoring is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.

Reconnaissance

Reconnaissance is the phase of an attack where an attackers finds new systems, maps out networks, and probes for specific, exploitable vulnerabilities.

Reflexive ACLs (Cisco)

Reflexive ACLs for Cisco routers are a step towards making the router act like a stateful firewall. The router will make filtering decisions based on whether connections are a part of established traffic or not.

Registry

The Registry in Windows operating systems in the central set of settings and information required to run the Windows computer.

Regression Analysis

The use of scripted tests which are used to test software for all possible input is should expect. Typically developers will create a set of regression tests that are executed before a new version of a software is released. Also see “fuzzing”.

Request for Comment (RFC)

A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.

Resource Exhaustion

Resource exhaustion attacks involve tying up finite resources on a system, making them unavailable to others.

Response

A response is information sent that is responding to some stimulus.

Reverse Engineering

Acquiring sensitive data by disassembling and analyzing the design of a system component.

Reverse Lookup

Find out the hostname that corresponds to a particular IP address. Reverse lookup uses an IP (Internet Protocol) address to find a domain name.

Reverse Proxy

Reverse proxies take public HTTP requests and pass them to back-end webservers to send the content to it, so the proxy can then send the content to the end-user.

Risk

Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Risk Assessment

A Risk Assessment is the process by which risks are identified and the impact of those risks determined.

Risk Averse

Avoiding risk even if this leads to the loss of opportunity. For example, using a (more expensive) phone call vs. sending an e-mail in order to avoid risks associated with e-mail may be considered “Risk Averse”

Rivest-Shamir-Adleman (RSA)

An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

Role Based Access Control

Role based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.

Root

Root is the name of the administrator account in Unix systems.

“God is present in every Jiva; there is no other God besides that. Who serves Jiva serves God indeed.”

Root kit

A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.

Router

Routers interconnect logical networks by forwarding information to other networks based upon IP addresses.

Routing Information Protocol (RIP)

Routing Information Protocol is a distance vector protocol used for interior gateway routing which uses hop count as the sole metric of a path's cost.

Routing Loop

A routing loop is where two or more poorly configured routers repeatedly exchange the same packet over and over.

RPC Scans

RPC scans determine which RPC services are running on a machine.

Rule Set Based Access Control (RSBAC)

Rule Set Based Access Control targets actions based on rules for entities operating on objects.

S/Key

A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.

Safety

Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

Scavenging

Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

Secure Electronic Transactions (SET)

Secure Electronic Transactions is a protocol developed for credit card transactions in which all parties (customers, merchant, and bank) are authenticated using digital signatures, encryption protects the message and provides integrity, and provides end-to-end security for credit card transactions online.

Secure Shell (SSH)

A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Secure Sockets Layer (SSL)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Security Policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Segment

Segment is another name for TCP packets.

Sensitive Information

Sensitive information, as defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.

Separation of Duties

Separation of duties is the principle of splitting privileges among multiple individuals or systems.

Server

A system entity that provides a service in response to requests from other system entities called clients.

Session

A session is a virtual connection between two hosts by which network traffic is passed.

Session Hijacking

Take over a session that someone else has established.

Session Key

In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

SHAL

A one way cryptographic hash function. Also see "MD5"

Shadow Password Files

A system file in which encryption user password are stored so that they aren't available to people who try to break into the system.

Share

A share is a resource made public on a machine, such as a directory (file share) or printer (printer share).

Shell

A Unix term for the interactive user interface with an operating system. The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called a command interpreter. A shell usually implies an interface with a command syntax (think of the DOS operating system and its "C:>" prompts and user commands such as "dir" and "edit").

Signals Analysis

Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Signature

A Signature is a distinct pattern in network traffic that can be identified to a specific tool or exploit.

Simple Integrity Property

In Simple Integrity Property a user cannot write data to a higher integrity level than their own.

Simple Network Management Protocol (SNMP)

The protocol governing network management and the monitoring of network devices and their functions. A set of protocols for managing complex networks.

Simple Security Property

In Simple Security Property a user cannot read data of a higher classification than their own.

Skimming

Skimming is the capturing of personal information on the credit card by using skimming device to scan the card details on the magnetic strip.

Smartcard

A smartcard is an electronic badge that includes a magnetic strip or chip that can record and replay a set key.

Smurf

The Smurf attack works by spoofing the target address and sending a ping to the broadcast address for a remote network, which results in a large amount of ping replies being sent to the target.

Sniffer

A sniffer is a tool that monitors network traffic as it received in a network interface.

Sniffing

A synonym for "passive wiretapping."

Social Engineering

A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems.

*Truth stands, even if there be no public support. It is self-sustained. - **Mahatma Gandhi***

Socket

The socket tells a host's IP stack where to plug in a data stream so that it connects to the right application.

Socket Pair

A way to uniquely specify a connection, i.e., source IP address, source port, destination IP address, destination port.

SOCKS

A protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. SOCKS uses sockets to represent and keep track of individual connections. The client side of SOCKS is built into certain Web browsers and the server side can be added to a proxy server.

Software

Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Source Port

The port that a host uses to connect to a server. It is usually a number greater than or equal to 1024. It is randomly generated and is different each time a connection is made.

Spam

Electronic junk mail or junk newsgroup postings.

Spanning Port

Configures the switch to behave like a hub for a specific port.

Split Horizon

Split horizon is a algorithm for avoiding problems caused by including routes in updates sent to the gateway from which they were learned.

Split Key

A cryptographic key that is divided into two or more separate data items that individually convey no knowledge of the whole key that results from combining the items.

Spoof

Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

SQL Injection

SQL injection is a type of input validation attack specific to database-driven applications where SQL code is inserted into application queries to manipulate the database.

Stack Mashing

Stack mashing is the technique of using a buffer overflow to trick a computer into executing arbitrary code.

Standard ACLs (Cisco)

Standard ACLs on Cisco routers make packet filtering decisions based on Source IP address only.

Star Property

In Star Property, a user cannot write data to a lower classification level without logging in at that lower classification level.

State Machine

A system that moves through a series of progressive conditions.

Stateful Inspection

Also referred to as dynamic packet filtering. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

Static Host Tables

Static host tables are text files that contain hostname and address mapping.

Static Routing

Static routing means that routing table entries contain information that does not change.

Stealthing

Stealthing is a term that refers to approaches used by malicious code to conceal its presence on the infected system.

Steganalysis

Steganalysis is the process of detecting and defeating the use of steganography.

Steganography

Methods of hiding the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself. An example of a steganographic method is “invisible” ink.

Stimulus

Stimulus is network traffic that initiates a connection or solicits a response.

Store-and-Forward

Store-and-Forward is a method of switching where the entire packet is read by a switch to determine if it is intact before forwarding it.

Straight-Through Cable

A straight-through cable is where the pins on one side of the connector are wired to the same pins on the other end. It is used for interconnecting nodes on the network.

Stream Cipher

A stream cipher works by encryption a message a single bit, byte, or computer word at a time.

Strong Star Property

In Strong Star Property, a user cannot write data to higher or lower classifications levels than their own.

Sub Network

A separately identifiable part of a larger network that typically represents a certain limited number of host computers, the hosts in a building or geographic area, or the hosts on an individual local area network.

Subnet Mask

A subnet mask (or number) is used to determine the number of bits used for the subnet and host portions of the address. The mask is a 32-bit value that uses one-bits for the network and subnet portions and zero-bits for the host portion.

Subscription Encryption

In subscription encryption, the message is encrypted by substituting one character for another. In the most basic form, this involves replacing and rotating each character by a certain number of letters of the alphabet.

Switch

A switch is a networking device that keeps track of MAC addresses attached to each of its ports so that data is only transmitted on the ports that are the intended recipient of the data.

Switched Network

A communications network, such as the public switched telephone network, in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices. Any network providing switched communications service.

Symbolic Links

Special files which point at another file.

Symmetric Cryptography

A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key.

Symmetric Key

A cryptographic key that is used in a symmetric cryptographic algorithm.

SYN Flood

A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

Synchronization

Synchronization is the signal made up of a distinctive pattern of bits that network hardware looks for to signal that start of a frame.

Syslog

Syslog is the system logging facility for UNIX systems.

System Interference

System interference is defined as the serious hindering, without right, of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

System Security Officer (SSO)

A person responsible for enforcement or administration of the security policy that applies to the system.

System-Specific Policy

A System-specific policy is a policy written for a specific system or device.

T1, T3

A digital circuit using TDM (Time-Division Multiplexing).

Tamper

To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

TCP Fingerprinting

TCP fingerprinting is the user of odd packet header combinations to determine a remote operating system.

TCP Full Open Scan

TCP Full Open scans check each port by performing a full three-way handshake on each port to determine if it was open.

TCP Half Open Scan

TCP Half Open scans work by performing the first half of a three-way handshake to determine if a port is open.

TCP Wrapper

A software package which can be used to restrict access to certain network services based on the source of the connection; a simple tool to monitor and control incoming network traffic.

TCP/IP

A synonym for "Internet Protocol Suite;" in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).

TCPDump

TCPDump is a freeware protocol analyzer for Unix that can monitor network traffic on a wire.

TELNET

A TCP-based, application-layer, Internet Standard protocol for remote login from one host to another.

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Threat Assessment

A threat assessment is the identification of types of threats that an organization might be exposed to.

Threat Model

A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.

Threat Vector

The method a threat uses to get to the target.

Time to Live

A value in an Internet Protocol packet that tells a network router whether or not the packet has been in the network too long and should be discarded.

Token Ring

A token ring network is a local area network in which all computers are connected in a ring or star topology and a binary digit or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time.

Token-Based Access Control

Token based access control associates a list of objects and their privileges with each user. (The opposite of list based.)

Token-Based Devices

A token-based device is triggered by the time of day, so every minute the password changes, requiring the user to have the token with them when they log in.

Topology

The geometric arrangement of a computer system. Common topologies include a bus, star, and ring. The specific physical, i.e., real, or logical, i.e., virtual, arrangement of the elements of a network. Note 1: Two networks have the same topology if the connection configuration is the same, although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types. Note 2: The common types of network topology are illustrated

Trace Route (tracert.exe)

Trace route is a tool the maps the route a packet takes from the local machine to a remote destination.

Transmission Control Protocol (TCP)

A set of rules (protocol) used along with the Internet Protocol to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Transport Layer Security (TLS)

A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.

Triple DES

A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

Triple-Wrapped

S/MIME usage: data that has been signed with a digital signature, and then encrypted, and then signed again.

Trojan Horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Trunking

Trunking is connecting switched together so that they can share VLAN information between them.

Trust

Trust determine which permissions and what actions other systems or users can perform on remote machines.

Trusted Ports

Trusted ports are ports below number 1024 usually allowed to be opened by the root user.

"By doing well the duty which is nearest to us, the duty which is in our hands, we make ourselves stronger"

Tunnel

A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. Most often, a tunnel is a logical point-to-point link - i.e., an OSI layer 2 connection - created by encapsulating the layer 2 protocol in a transport protocol (such as TCP), in a network or inter-network layer protocol (such as IP), or in another link layer protocol. Tunnelling can move data between computers that use a protocol not supported by the network connecting them.

UDP Scan

UDP scans perform scans to determine which UDP ports are open.

Unicast

Broadcasting from host to host.

Uniform Resource Identifier (URI)

The generic term for all types of names and addresses that refer to objects on the World Wide Web.

Uniform Resource Locator (URL)

The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, http://www.pcwebopedia.com/index.html.

Unix

A popular multi-user, multitasking operating system developed at Bell Labs in the early 1970s. Created by just a handful of programrs, UNIX was designed to be a small, flexible system used exclusively by programrs.

Unprotected Share

In Windows terminology, a "share" is a mechanism that allows a user to connect to file systems and printers on other systems. An "unprotected share" is one that allows anyone to connect to it.

Unsolicited Commercial Communications

A communication in any form with commercial content that is sent to a recipient who has not requested data.

User

A person, organization entity, or automated process that accesses a system, whether authorized to do so or not.

User Contingency Plan

User contingency plan is the alternative methods of continuing business operations if IT systems are unavailable.

"Do not judge me by my successes, judge me by how many times I fell down and got back up again."

User Datagram Protocol (UDP)

A communications protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagram's over an IP network. It's used primarily for broadcasting messages over a network. UDP uses the Internet Protocol to get a datagram from one computer to another but does not divide a message into packets (datagram's) and reassemble it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in.

Virtual Private Network (VPN)

A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunnelling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall; the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

Virus

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Vishing

The term 'vishing' coined from the words voice and phishing, is the criminal practice of using voice over phone systems to gain access to details about account numbers, PIN date of birth and expiry date of credit card holders and using it for fraudulent activities.

Voice Firewall

A physical discontinuity in a voice network that monitors, alerts and controls inbound and outbound voice network activity based on user-defined call admission control (CAC) policies, voice application layer security threats or unauthorized service use violations.

Voice Intrusion Prevention System (IPS)

Voice IPS is a security management system for voice networks which monitors voice traffic for multiple calling patterns or attack/abuse signatures to proactively detect and prevent toll fraud, Denial of Service, telecom attacks, service abuse, and other anomalous activity.

War Chalking

War chalking is marking areas, usually on sidewalks with chalk, that receive wireless signals that can be accessed.

War Dialer

A computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break into the systems.

War Dialing

War dialing is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise in an attempt to circumvent perimeter security.

War Driving

War driving is the process of travelling around looking for wireless access point signals that can be used to get network access.

Web of Trust

A web of trust is the trust that naturally evolves as a user starts to trust other's signatures, and the signatures that they trust.

Web Server

A software process that runs on a host computer connected to the Internet to respond to HTTP requests for documents from client web browsers.

WHOIS

An IP for finding information about resources on networks.

Windump

Windump is a freeware tool for Windows that is a protocol analyzer that can monitor network traffic on a wire.

Wired Equivalent Privacy (WEP)

A security protocol for wireless local area networks defined in the standard IEEE 802.11b.

Wireless Application Protocol

A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat.

Wiretapping

Monitoring and recording data that is flowing between two points in a communication system.

World Wide Web ("the Web", WWW, W3)

The global, hypermedia-based collection of information and services that is available on Internet servers and is accessed by browsers using Hypertext Transfer Protocol and other information retrieval mechanisms.

Worm

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Zero Day

The "Day Zero" or "Zero Day" is the day a new vulnerability is made known. In some cases, a "zero days" exploit is referred to an exploit for which no patch is available yet. ("day one" - day at which the patch is made available).

Zero-day Attack

A zero-day (or zero-hour or day zero) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software developer knows about the vulnerability.

Zombies

A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.