CHAPTER – VII

PREVENTIVE MEASURES IN RESPECT OF CYBER CRIMES

Cyber crime is emerging as a serious threat. Increasing use of the internet had simultaneously given birth to innovative ways for committing crimes that had no boundary. Many cyber crimes went unreported due to reluctance or ignorance on the part of the victims. As a result, reliable statistics on crimes were not available for assessing the extent of the problem. World wide governments, police departments and intelligence units have started to react. Initiatives to curb cross-border cyber threats are taking shape. Cyber crime cells across the country have been formed by the Police Department in all the States of India and have started educating the personnel.¹

Data are more valuable than money. Once spent, money is gone, but data can be used and reused to produce more money. The ability to reuse data to access on-line banking applications, authorize and activate credit cards, or access organization networks has enabled cyber criminals to create an extensive archive of data for ongoing illicit activities.²

The trend has been changed from individuals operating for mischief or profit to international organised crime groups carrying out criminal activities such as terrorism, money laundering, drug trafficking, cyber based extortion and fraud, child pornography and spreading hatred. Hence, understanding the changes in crime patterns is critical to take preventive steps.³

¹ Criminal Investigation Department Review – January 2008 – Article on “Cyber Crime Scenario in India” submitted by Dr.B.Muthukumaran, Chief Consultant, Gemini Communication Limited, p.17.
Cyber Space Security Management has already become an important component of National Security Management of Military-related Scientific Security Management and Intelligence Management all over the world. Future intrusions threatening our national security may not necessarily come from across the land frontier, or in air space or across maritime waters, but happen in cyberspace. Intelligence operations and covert actions will increasingly become cyber-based. It is important that our intelligence agencies gear themselves up to this new threat. It is, therefore, necessary to put in place a ‘National Cyber Space Security Management Policy’ to define the tasks, specify responsibilities of individual agencies with an integrated architecture.

**International Initiatives to Combat Cyber Crimes**

At the international level attempts have been made to harmonise the principles and laws applicable to cyberspace to combat the menace of cyber crimes. In recent years, certain international bodies, such as the Council of Europe, the Organisation for Economic Co-operation and Development (OECD), or the G8 Conference, have begun to consider cyber security and cyber crime issues as a part of their policy agenda. Whilst this has included extending co-operation on terrorism and security, an equally important strand in these discussions has been the development of policies on ‘information systems’. The purpose of this policy discussion was to develop a common global standard for the retention of telecommunications and internet traffic data. For example, during the

---

G8 Conference in 1998, a set of principles and a ten point action plan were adopted to ‘preserve electronic data’ for sharing between ‘international partners’.\(^5\)

Today’s stunning cyber-crime trends demand a strong, bold, near-term response.

Several additional developments have heightened the current cyber crime wave:\(^6\)

1. Social networking and constant online communication – and the proliferation of communication devices, networks, and users – have generated new vulnerabilities that create more cyber crime opportunities.

2. Online banking, investing, retail and wholesale trade, and intellectual property distribution present countless opportunities for theft, fraud, misdirection, misappropriation, and other cyber crimes.

3. Foreign rogue governments, terrorist organizations, and related acts, sometimes exploit the cyber vulnerabilities to help fund their espionage, warfare, and terror campaigns.

4. Organized crime has extended its reach into cyberspace, adding cyber crime to its portfolio of “businesses”.

5. Economic hardships spawned by the 2008-09 recession may generate resentment and financial motivations that can drive internal parties or former employees to crime. In fact, “wire mule” may be a new job opportunity in the emerging “new economy”.

---


\(^6\) [www.deloitte.com](http://www.deloitte.com)
Role of Government

The Information Technology’s infrastructures to the country have gained visibility in the recent years due to cyber attacks and rapid growth in identity theft and financial frauds. These events have made it increasingly clear that the security of the IT infrastructure has become a key strategic interest to the Government. Although the industry now making investments in security-related infrastructure, their actions are directed primarily at short-term efforts driven by market demands to address immediate security problems.\(^7\)

The Government has a different but equally important role to play in cyber security assurance in the form of long-term strategies. In this direction, the deliberations of the National Information Board (NIB), National Security Council (NSC) have stressed the importance of a national strategy on cyber security, development of national capabilities for ensuring adequate protection of critical information infrastructure including rapid response and remediation to security incidents, long term investments in infrastructure facilities, capacity building and R&D. Government responsibilities in long-term investment and fundamental research will enable development of new concepts, technologies, infrastructure prototypes, and trained personnel needed to spur on next-generation security solutions.

Government leadership catalyzes activities of strategic importance to the Nation. In cyber security assurance, such leadership can energize a broad collaboration with private-sector partners and stakeholders to generate fundamental technological advances in the security of the nation’s IT

\(^7\) http://deity.gov.in browsed on 30\(^{th}\) September 2013.
infrastructure. First, in support of national and economic security, the Government should identify the most dangerous classes of cyber security assurance threats to the Nation, the most critical IT infrastructure vulnerabilities, and the most difficult cyber security assurance problems. Second, the Government can use these findings to develop and implement a coordinated R&D effort focused on the key research needs that can only be addressed with such leadership. While these needs will evolve over time, this Cyber Security Strategy provides a starting point for such an effort.

Public-private partnership is a key component of Cyber Security Strategy. These partnerships can usefully confront coordination problems. They can significantly enhance information exchange and cooperation. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

**SOCIETY RESPONSE**

The war against hacking is a continuous battle that has a starting point with no end at all. The world is using a variety of methods either to halt attacks or minimize their effects on society. The best way to minimise the effect of attacks or even avoid them is by building a well educated computer user who can gain benefit from different security techniques in the war against hacking. It is believed that the first step to allocate hacking activities should be by applying information security policies and nowadays policies are running in a large number of organisations, these policies imply that all employees should sign a work place behaviour sheet specially the ones dealing with sensitive data and information that must be kept secret. According to those policies any employee who is caught
guilty and participating in information theft or hacking will be questioned and further sanctions are applied. The companies are making a big mistake by waiting for the attack to happen then when it is too late they reconsider their security techniques and by hiding the attacks on their system and should inform authorities about any incident to help in tracking hackers and intruders.

Regarding security software, different opinions agree that there is no total security and the more sophisticated security tools are invented more technical hacking attacks are applied, that is because hacking is a big field with no limitations, and hackers are inventing new techniques at a rate faster than security utilities, even with the availability of security tools, it is hard to fill all holes. Computer users for the inefficiency of security tools, having a security software is not a solution by itself, users should realise that they need those tools and should learn how and when to use them.

The hacking will never fade away, but it can be managed if precautions are taken and there will never be total security. And till this moment, we are suffering from hacking attacks almost on daily basis and the only thing we can do is to minimise their effects and rarely prevent them from happening.

The technological futurism is the subject of much political controversy and manoeuvring at the current time, it seems likely though, that the new government administration will lead out more liberalisation to support competition-led innovation and technological advances in communications media, and there is a clear emphasis on the use of technology for economic development in the shaping of public policy statements.
Prevention of Cyber Crime

1. To prevent cyber stalking, disclosing of any information pertaining to any one should be avoided. This is as good as not disclosing your identity to strangers in public place.

2. Sending any photograph online particularly to strangers should be avoided and chat friends as there have been incidents of misuse of the photographs.

3. Latest and updated anti-virus software to guard against virus attacks should be sued.

4. Backing up volumes from the computer should be done periodically, so that one may not suffer data loss in case of virus contamination.

5. The credit card number should not be sent to any site that is not secured, to guard against frauds.

6. Keeping a watch on the sites that the children are accessing should be done to prevent any kind of harassment or depravation in children.

7. It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

8. Website owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.

10. Web servers running public sites must be physically separately protected from internal corporate network.  

**Technical Measures to combat Cyber Crime**

Cyber crime undoubtedly is a technical crime. Hence, technical measures are equally important to tackle this crime.  

Cryptography is not new; armies were using it since times immemorial and it is supposed to be 3500 years old. Now business organizations have started using cryptography. Cryptography involves coding the text of a message using other letters or figures by using different algorithms and making the content meaningless for anybody intercepting these messages. The content of the message can only be deciphered by the person having the key to decode the message. A big problem in e-commerce is repudiation. Digital signatures and Digital certificates are an effort to overcome this problem. Digital signatures are based on asymmetric cryptography. Digital documents are signed by attaching certain encrypted data onto it, which cannot be repudiated later by the person signing. Digital certificates are the electronic certificates issued by ‘certification authorities’ who vouch for the authenticity of the digital signature that is being used in a transaction. Many countries have enacted laws permitting use of digital signatures in commercial activities. Cryptography and Digital signatures can be very effective guards against cyber crime.

---

8 Criminal Investigation Department Review – January 2008 – Article on “Types of Cyber Crime – An Overview” submitted by Mr. Syed Umarathab, UGC Doctoral Research Fellow, Department of Criminology, University of Madras, p.13.

COMPUTER SECURITY

Securing your computer, networks with a strong password and regularly scan computers for backdoors, keyloggers, Root Kits etc., Monitoring network for unauthorised access to your network of your system is the computer security.¹⁰

NETWORK FIREWALLS

Several technologies to protect network traffic with authentication and encryption were introduced. Firewalls use a different approach: they block harmful network traffic from spreading to private networks and computers. A firewall itself is a piece of software or a hardware device used as a filter to block harmful network traffic. A server machine can also be configured to host firewall software to protect private networks. When properly configured, firewalls can be used to protect private networks from the threats caused by hackers and viruses:

1. Firewalls can protect servers from denial-of-service attacks.
2. Firewalls can block hackers from accessing network-based application software.
3. Firewalls can be used to stop e-mail spam.
4. Firewalls can be used to prevent hackers from logging on to the computers in a private network.
5. Firewalls can be used to check the content of macros, which may be used by hackers to steal sensitive information or cause a system to crash.
6. Firewalls can prevent computer virus infection.¹¹

Safety Tips to Protect Your Computer

Following are some safety tips to protect you from Keyloggers, Trojans and Spyware:

1. As a common practice, suspicious or unsolicited emails (spam emails) should not be opened and that be deleted from inbox.

2. Even if a spam email is opened, under any circumstances, any links, or any files attached to them should not be opened or downloaded.

3. Very good anti-virus software should be installed on the computer that not only protects the computer from viruses, but also from unwanted programs. Any latest versions of the software may be updated.

4. Automatic updates/firewall should be turned on and the security patches should be downloaded for windows system.

5. While accessing websites that provide free downloads (such as music, serial keys, adult content, games, movies etc), we should be varied. They may install harmful programs without our knowledge.

6. The software that auto-completes online forms on the computer should not be used. This can give internet scammers easy access to our personal and credit card details.

7. While downloading files from the internet, it should be made sure that it is from a known or reputed source. If the file is an executable application (for example, if the file name ends with
“.exe”) and it should be confirmed that exactly what the application will do.

8. If a pop-up screen appears on the screen and prompts you for an action (for example if it asks you to ‘Agree’ or ‘Accept’ something will be shown), then be sure to read the text in the pop-up screen and any terms and conditions carefully and only when confirming the safety, action should be taken.

9. Various security-related technologies have been invented to protect network traffic. Six of them were discussed including Intrusion Detection System (IDS), IP Security (IPSec), Remote Authentication Dial In User Service (RADIUS), Secure Shell (SSH), Secure Socket Layer (SSL) and Wi-Fi Protected Access (WPA). These technologies provide the mechanisms for data encryption, user and computer authentication and network monitoring.

10. Firewalls are the first defense for protecting a network. The issues related to firewall rules are discussed. The firewall rules can be set up based on the network services, related communication ports, protocols, data content and connection states. Various types of firewalls have been introduced to implement firewall rules. Properly placing a firewall in a network system can significantly affect the effectiveness of the firewall.12

---

Protection from Malicious Code and Hacker Attacks

There are several steps you can take to protect your computer from today’s cyber threats. Following the simple guidelines below will help minimise the risk of attack.

1. Computer should be protected by installing Internet security software.
2. Regular updation should be done regularly (i.e. at least once a day).
3. Security patches should be installed for operating system and applications. Automatic updation should be made for Windows and Microsoft Office.
4. Other applications should be updated.
5. If an e-mail with an attached file (Word documents, Excel spreadsheets, EXE files, etc.) is received, it should not be opened unless it is confirmed that who sent it and attachment should not be opened in an unsolicited (spam) e-mail. The same is true for e-mail messages or IM (Instant Messaging) messages that contain links.
6. For installation of software is needed, computer’s Administrator account only to be used. For everyday, a separate account with only limited access rights should be created and used (this can be using User Accounts in Control Panel). The same is true for e-mail messages or IM (Instant Messaging) messages that contain links.
7. Data Backup should be taken regularly to a CD, DVD, or external USB drive. If the files have been damaged or encrypted by a malicious programme, that should be copied from the backup.¹³

**Approaches of Filtering**

Filter software is increasingly used by a wide variety of groups in society and in many societies, its use is mandated by law. Filter software is used in the home and school markets. Parents and teachers use a filter to prevent children from accessing content deemed not suitable for them. Sexually explicit and violent material is of most concern to parents and teachers. The regulation of controversial material in respect to children is also an issue. Recently the corporate world has embraced filter technology because of concerns expressed about loss of productivity and risks of litigation.

Filter software is designed to block access to controversial Internet content. Such content can be blocked in three places: at the source (that is the provider or creator of the content); in transit either at the application level or at the packet level; at the receiver. Blocking at the receiver end may be done directly by installation of a filter on the receiver’s PC, or indirectly at the receiver’s Internet Service Provider (ISP) with a subscription to a “white list”. The process of blocking requires that the content must be rated based on some classification system. Such a system may be a simple one on which produces a rating of allowed/disallowed, or a sophisticated one like the Platform for Internet Content Selection (PICS) that employs many categories and values.¹⁴

---

¹³ www.caspersky.co.in browsed on 23rd May 2014.
Ethical Hacking

Ethical hacking is identifying vulnerabilities through the art of exploitation. Prying open holes in systems and applications helps to determine the state of security within an organization. It exposes weaknesses in operating systems, services, applications, and even users for the betterment of the company and its business.

Ethical hacking has become a very popular security activity. It seems everyone is looking to hack their networks to see what gaping holes they will find this quarter. Tests are being performed all over the world in many different ways, using different methods, different tools, and very different assumptions of success and failure.

A hacker only has to find one hole to meet the objective, whereas the security technology and the people who support it have to defend against all points of entry, even the authorized ones, at times. Always being on the defensive requires intense intellect, diligence, and tenacity, arguably more so than an attacker. The goal is to not abandon these disadvantages and attempt to fully imitate a hacker. Simply approach an ethical hack – as a customer or consultant – fully aware of your disadvantages and limitations, and understand how to best work with them. The apparent differences need to be embraced and used as a benefit and a tool to bring value to the engagement.15

HACKED PASSWORDS

Top ten most popular passwords (in that order) from among 32 million hacked passwords from RockYou.com\(^\text{16}\):

123456, 12345, 123456789, Password, iloveyou, princess, rockyou, 1234567, 12345678, abc123.

GOOD PASSWORD PRACTICES

1. It should contain at least eight characters.\(^\text{17}\)

2. It should contain a mix of four different types of characters—upper case letters, lower case letters, numbers, and special characters such as # $ % & * , ; ” If there is only one letter or special character, it should not be either the first or last character in the password.

3. It should not be a name, a slang word, or any word in the dictionary. It should not include any part of your name or your e-mail address.

Ditalee, Ditalee1, Ditaloo3, iambhiku, pareekshanh84, *sha1973******, peter1, hemant, love25786, 080176, kingoforkut.

WORST PASSWORD PRACTICES

1. About 30% of users chose passwords whose length is equal or below six characters.\(^\text{18}\)

2. Moreover, almost 60% of users chose their passwords from a limited set of alpha-numeric characters.

\(^{16}\) www.rockyou.com browsed on 23\(^\text{rd}\) May 2011.
\(^{17}\) Ibid.
\(^{18}\) Ibid.
3. Nearly 50% of users used names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on).

**Awareness on Cyber Crime**

Awareness activities should also take into account the characteristics of different environments, such as those encountered by telecommuters and traveling employees in hotels, coffee shops, and other external locations. Examples of such practices are as follows:

1. Not opening suspicious e-mails or e-mail attachments from unknown or known senders.
2. Not clicking on suspicious web browser popup windows.
3. Not visiting web sites that are at least somewhat likely to contain malicious content.
4. Not opening files with file extensions that are likely to be associated with malware.
5. Not disabling the additional security control mechanisms.
6. Not using administrator-level accounts for regular system operation.
7. Not downloading or executing applications from untrusted sources.

**Mobile Phones**

The mobile communication is naturally a target for all the threats that occur in fixed network communication, i.e., mosquered identities, authorization violations, eavesdropping, data loss, modified and falsified data units, repudiation

---

of communication processes and sabotage. Consequently, similar measures as in fixed networks should be taken mobile communication works.\textsuperscript{20}

\textbf{E-Security Tips (Internet)}

- Harmful communications (emails, chat logs, posts etc) should not be deleted. These may help provide vital information about the identity of the person behind these.
- Not to be panic.
- Any immediate physical danger of bodily harm is felt, local police should be called.
- Getting into huge arguments online during chat or discussions with other users should be avoided.
- It should be remembered that all other internet users are strangers and who we are chatting with. So it should be careful and polite.
- While sharing personal information about yourself online, extreme care should be taken.
- The chatting nickname should be chosen carefully so as not to offend others.
- Personal information in public spaces anywhere online should not be showed with strangers including in e-mail. Personal information as part of any user profile should not be posted.
- While meeting online acquaintances in person, extreme caution should be taken while choosing to meet, should be taken along a friend.

• This is to make sure that ISP and Internet Relay Chart (IRC) network have an acceptable use policy that prohibits cyber-stalking. And if the network fails to respond to the complaints, switching to a provider that is more responsive to user complaints should be considered.

• If a situation online becomes hostile, the system should be logged off and the assistance of local police should be drawn if the situation takes place in fear.\(^{21}\)

• All communications should be saved for evidence and not to be edited in anyway.

Safety Tips for Mobile Phone Users

1. Phone’s security lock code should be used, if it has one.\(^{22}\)

2. Bluetooth should be disabled, if not in use.

3. Mobile hanging ribbon/thread/strip to be used always for safety.

4. Anti-virus software should be installed.

5. Details of our Electronic Serial Number (ESN) of CDMA phone to be recorded.

6. Separate insurance should be considered.

7. GSM phone have a unique IMEI number. To find the records of our mobile phone, *#106# should be typed and it should be kept safe.

8. Marking our phone with the postcode would help the police identify as stolen ones.

---

\(^{21}\) www.cbcid.tn.nic.in browsed on 25\(^{th}\) December 2010.

\(^{22}\) Ibid.
9. PIN Code on the handset should be enabled.

10. The phone should be unlocked when using it.

11. Without knowing the seller is the owner, the mobile phone should not be bought and the original bill of purchased to be asked.

12. If the phone is lost or stolen, the same to be complained to the police immediately and the acknowledgement should be received.

13. The Service Provider should be informed if your phone is stolen or lost.

14. When the phone is not in use, it should be kept in pocket or bag for want of out of sight of others and it should not be attracted others while carrying it in the street.

15. The mobile phone should not be left unattended.

16. The windows of the house and doors of the door should be closed while we are talking on mobile phone.

17. While driving, the cell phone should not be kept on the dashboard.

18. Mobile Tracking Service available in the Mobile Market should be subscribed (if it is supported on our handset).

19. Extra vigilance to be taken for results.

20. Forwarding of any content, which is pornographic in nature is a punishable offence and we should be alert on that.
ATM Security Tips to Prevent Frauds

1. Confidentiality of card information is should be maintained at the time of transaction.\(^{23}\)

2. At the time of transacting, we should ensure that no one is standing for visible of our transaction. Our body should be used as a shield if necessary, while entering the Personal Identification Number (PIN).

3. ATM PIN of Credit card/Debit card should be changed at regular intervals.

4. In case ATM requires more time while transacting, the required instructions given by the ATM should be followed and the assistance of any strangers should not be sought.

5. The PIN number should be in memory. It should not be written on the wallet of the ATM card and PIN number should not be disclosed to anyone (including bank employees).

6. After completion of transaction, it should not forget to collect back the card from ATM.

7. If the card is captured by ATM, the cancel button should be used couple of times for checking whether the card comes out. If not, a complaint should be made with the nearest Bank Branch or Phone Banking should be called.

8. Avoid speaking on the mobile, while you are transacting.

---

\(^{23}\) Pamphlet issued by HDFC Bank.
9. If anything strange/suspicious in the ATM centre or ATM machine is noticed, the security personnel should be informed and should be left from the ATM. Even the transaction is already started, it should be cancelled.

**Safety Tips for using Social Networking Sites**

1. Posting of personal information on the social networking sites should be limited. Post of information that would make us vulnerable, it should be avoided (e.g. our address, information about our schedule or routine).

2. The internet is a public resource, that should be remembered – posting information will be seen by anyone. This includes information in our profile and in blogs and other forums. Also, once information is posted online, the same will not be retracted. Even if we remove the information from a site, saved or cached versions may still exist on other people’s machines.

3. The internet makes it easy to people to misrepresent their identities and motives. Limiting the people who are allowed to contact us on these sites should be limited. If interaction with other people, we should be cautious about the amount of information we reveal or agreeing to meet them in person since we do not know them directly.

---

4. We should not believe everything which we read online and we should be skeptical, since people may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, a product of exaggeration, or a joke. Appropriate precaution should be taken to verify the authenticity of any information before taking any action.

5. Privacy policies should be check, since some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, location of the policy for handling referrals should be verified to make sure that we do not unintentionally sign our friends up for spam. Some sites will continue to send email messages to anyone to refer us until they join.

Safety Tips to Avoid Online Shopping Frauds

1. We should aware of phishing and the receiving emails should be verified whether it is coming from the correct source and that we are logging in at the correct website.²⁵

2. When making payment, prefer using your credit card over online transfer. Using a credit card give you the opportunity of a chargeback in case the transaction turns out a fraud.

3. After trusting the seller only, we should use debit card, wire transfer, or money order.

4. Reputed escrow services should be used. An escrow service mediates a buyer and a seller. They accept money from buyers and release them to a seller only when the buyer confirms that the product was received to his/her satisfaction. But be wary of sellers or buyers who themselves pose as an escrow service to cheat the other – a buyer posing as an escrow service gets a product released without making payment, or a seller poses as an escrow service to trick the buyer from making a payment.

5. Feedbacks and rating of the buyer should be checked, which most online auction website provide.

6. Emails from outside of the auction website mentioning that the highest bidder has withdrawn and you are now entitled for a product should not be entertained. They veer us off the auction website and you lose any protection that the website may provide.

7. Deal with a seller outside the auction should not be made. Although they sound lucrative, we are at a very high risk of being cheated.

8. The terms and conditions of website’s terms and conditions, buyer protection policy, refund policy before making a transaction should be thoroughly read. Here, they list in how many days the order will be fulfilled, what if the product you receive is not the same as what was advertised, and so on. The policies are fair on both buyers and sellers should also be checked.
9. While purchasing the product, we have to check that it has appropriate warranty and the concerned documentation. If not, we intend to purchase it without that protection. Shipping and delivery is covered by the seller should be checked or if we have to bear those costs.

10. While purchasing a product, we should check that we are not allowed to possess lawfully.

11. BE WARY of products that offer revolutionary results. In most cases, they are fraudulent claims.

12. For emails that ask for your personal information, such as you login details or credit card details, we should not respond.

13. The online auction website for feedback on the seller should be read and a rating that they give to sellers and buyers. Most online auctions rate, the sellers and buyers would be based on their transaction’s feedback.

14. The product features and the model number that we intend to purchase should be read and we should verify these with what is being advertised by the seller.

15. When giving our credit card details or our debit account details at a website, we should check that the internet connection we are using is secure. The lock at the bottom or https (an ‘s’ appended to ‘http’) in the address field of your browser should be looked. These indicate that the connection is a secure one.
16. While making a transaction, we should avoid if anything in the auctions seems suspicious to you.

17. If we are cheated on any product purchase, we should be sure to post a note on the online auction website and let them know personally.

Role of Enterprises

Training employees/users in the proper role of computer security assures employee involvement/commitment. Disseminating the results of poor computer security – loss of customers, proprietary information, financial losses – motivates employees to be “computer security literate”.  

Educating employees on the use of computer security helps reduce errors and omissions. Communicating the penalties and/or actions that will be taken can also decrease the fraudulent actions and unauthorized activity of the disgruntled employee.

1. Technological Tools

Technology provides tools that may assist in preventing children from accessing inappropriate materials on the Internet or divulging personal information about themselves or their families online. The most common technological tools are “blocking” and “filtering” software, as described more fully below:

(a) Blocking Software

“Blocking” software uses a “bad site” list and prevents access to those sites. The vendor of the software identifies specified categories of words or

---

phrases that are deemed inappropriate and configures the blocking software to block sites on which the prohibited language appears. Although some vendors allow parents to customize the “bad site” list by allowing them to add or remove sites, others keep the list secret and do not permit parents to modify it.

Filtering Software

“Filtering” software blocks sites containing keywords, alone or in context with other keywords. Filtering software is available both directly and through some Internet service providers (ISPs) such as Lycos or Family Net.\(^27\)

Other Software

Other types of software enable parents to monitor and control their children’s use of the computer. For example, “monitoring and tracking” software allows parents to track how much time their children spend online, where their children go online, and how much time their children spend on the computer offline. “Outgoing filtering” software prevents children from sharing certain information with others over the Internet, such as their name, telephone number and address.\(^28\)

2. Non-technological Tools

(a) Parents to do

One of the most effective ways of protecting children from inappropriate material on the Internet is to teach them to use the Internet responsibly. Parents play a major role in this by taking responsibility for children’s online computer


There are certain safety tips parents can follow to ensure that their children use the Internet safely. These tips include:

- never give out personal information, such as home address, school name, or telephone number, in a public message such as a chat room or bulletin board;
- do not post photographs of children on websites or news groups that are available to the public;
- if a meeting is arranged, make the first one in a public place and be sure to accompany the child;
- never respond to messages that are suggestive, obscene, belligerent, threatening or make you feel uncomfortable;
- encourage children to tell you if they encounter such messages;
- report any inappropriate messages you receive immediately;
- consider keeping the computer in a room other than the child’s bedroom to monitor his or her online use;
- get to know your children’s online friends just as you get to know all of their other friends;
- set up specific rules for your children’s online use, such as the time of day and length of time that they can be online and appropriate sites for them to visit.
(b) Schools and Libraries to do

As increasing numbers of children have access to the Internet from their schools and neighbourhood libraries, we need to address the issue of how best to ensure that these children have positive, age-appropriate, educational online experiences.

School and libraries are currently using a wide range of technology tools and monitoring techniques to ensure that children do not encounter inappropriate material or dangerous situations while online.\textsuperscript{30}

**CYBER CRIME PREVENTION INITIATIVES OF CBCID**

In order to prevent computer crimes and create awareness among Internet users, the CB-CID has collaborated with NASSCOM (a non-profit representative body of Software and Service Companies) and organised ‘Cyber Safe Chennai Weeks’ in the years 2008 and 2009 so as to impart training to the police officers for effective investigation of cyber crimes. The CB CID officials have also contributed to public awareness by displaying posters at the Tamil Nadu Police Stall during the Annual Trade Fair organised by the Government of Tamil Nadu.

Each of the aforesaid characteristics of cyber crime ought to be considered while devising effective measures of checking, preventing and punishing cyber crimes which threaten the global community. Besides deterrent laws the following are the strategies which are required to be adopted simultaneously to deal with the menace of cyber crime.\textsuperscript{31}

(i) Since cyber crimes are crimes of technology, the law enforcement agencies ought to be trained in the intricacies of technology, so as to properly and effectively conduct investigations. A cyber cop has to be at least a half IT engineer to be a competent cyber crime investigator.

(ii) Since the cyber criminal has the tendency of jumping geographical borders, also called jurisdictional jumping, there has to be co-operation between law enforcement agencies of different countries.

(iii) Effective laws of extradition and their implementation are necessary to bring to trial cyber criminals across borders. These existing extradition treaties ought to be strengthened by co-operation in the International community.

(iv) The most effective weapon to counter cyber crime is the use of encryption and other security technologies. It has been said that we need better locks on computers and not on jails to prevent cyber crime.

(v) The IT industry must assume responsibility of protecting its own computer systems and networks by using secure technologies and should not depend upon the law enforcement agencies to track cyber criminals which is extremely difficulty to give anonymity provided by the Internet.
(vi) The Government should encourage the use of security technology and should work in close partnership with the private sector. It must facilitate and encourage research and development of new security technologies. Government should fund and support research and development and facilitate education about the measures to counter cyber crime.

(vii) Since most cyber crimes are not reported by victims in the Industry, it gives protection to cyber criminals. Cyber crimes are not reported by victims for fear of eroding the confidence and customers and the consequent loss of business. It needs to be understood that to suppress information about cyber crime having been victimized by cyber crime amounts to protection of, and encouraging cyber crime. The private sector must share information about cyber crime so as to understand its various forms and ways to deal with them more effectively.

(viii) Last, but not least, suggestion is that identification of citizens. Anonymity facilitates cyber crimes and thus must yield to the larger interest of the society. It is not being advocated that all contents and interactions on the Internet should be censored. Technological modes of easy identification of netizens in their interaction should be used only when necessary while investigating into allegations of cyber crime though privacy concerns are important, it has to be realized that identification of netizens in certain areas such as cyber crime is equally necessary.
The 5p Mantra of Cyber Cell, Mumbai Police

5p Mantra: Precaution, Prevention, Protection, Preservation and Perseverance.\textsuperscript{32}

WEB RATNA AWARD TO GOVERNMENT OF TAMIL NADU

Tamil Nadu Government bagged the Platinum Award in the Web Ratna Award 2009. This was awarded to Tamil Nadu Government and received by Mr.P.W.C.Davidar, Secretary, Information Technology, Government of Tamil Nadu, on 19\textsuperscript{th} April 2010 for the following projects included under the Comprehensive Web Presence category:

1. Government of Tamil Nadu Web Site
2. Anytime/Anywhere Land Records
3. E-Services for Transport
4. E-filing of VAT Returns
5. Online Medium, Small and Micro Enterprises
6. Online GDP Monitoring
7. Online GPF/Pension System
8. Tenders Information System
9. Tamil Nadu Text Books Online
10. Web GIS for District Planning
11. Monthly Public Distribution System Allotment Software
12. e-Attendance Monitoring System for Department of Technical Education.\textsuperscript{33}

\textsuperscript{32} http://cybercellmumbmai.gov.in browsed on 23\textsuperscript{rd} September 2014.
\textsuperscript{33} http://webratna.india.gov.in browsed on 14\textsuperscript{th} December 2014.