ITMR

योगः कर्मसु कौशलम्

WHITE PAPER ON

Cybercrime

Prepared by **Mohammed Samiuddin**

Contents

Cybercrime – Be(a)ware of the Nuisance

The concept of Cybercrime is not fundamentally different from the conventional crime. Both are based on the conduct, either by act or by omission that cause breach of law. Any criminal activity that uses a computer and the Internet, which includes sale of illegal articles, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyberstalking, pornography, downloading illegal video/audio files, hacking, developing and distributing viruses, posting confidential and personal information about others and transferring illegal funds comes within the ambit of Cybercrime.

Cybercrime is the latest and most intricate problem in the cyber space and has become a nuisance in the society. The increase in the usage of computers in several areas of social activity has increased attention to Cybercrimes. The widespread accessibility has further facilitated predatory personal crimes and property offenses, and greatly increased the potential victim and offender pools. The fact that the victim(s) can be depersonalized in the initial stages of an offense has also allowed some potential offenders to move more easily towards actual criminal behaviour.

Reasons for Cybercrime

"Human beings are vulnerable, so rule of law is required to protect them," says H L A Hart, a legal philosopher, in his work "The Concept of Law". Similarly, in the cyberspace, computers are vulnerable; so, to protect and safeguard them against cybercrime the rule of law is required. The reasons for cybercrime could be:

Less space to store more data

The unique characteristic of the computer is that it stores large data in a very small space. Therefore, the possibility to remove or derive information either through physical or virtual medium is much easier.

Loss of evidence

Loss of evidence is a very common problem as all data are routinely destroyed. Collection of data outside the territorial extent also paralyses this system of crime investigation further.

Reasons for Cybercrime

Accessibility

Guarding computers from unauthorised access is one of the major problems. The breach need not always be due to human error, it could also be the complex technology at times. Key loggers can steal access codes by secretly implanting logic bomb. The biometric systems can be fooled and even firewalls can be bypassed to get past the security system using advanced voice recorders, retina imagers, etc.

Laxity

Human behaviour and laxity are very closely connected. There is every chance for laxity while protecting the computer system and this in turn leaves way for a cyber-criminal to gain access and have a control over the computer system.

Complexity

The operating systems with which the computers work consist of millions of code. To err is human and so there could be a lag at any point of time. Cyber criminals can take advantage of this and enter the computer system.

Types of Cybercrime

Any crime committed using the Internet is cybercrime. There are many different types of which few are provided below:

- Hacking or Unauthorized Access – in this method a person hacks others computers without their knowledge. The hacker possesses very good knowledge on computers and computer programs
- Physical or Virtual Theft of Electronic Information stored in computer hard disks, removable storage media, etc.
- Spamming and Email bombarding: Spam is otherwise known as junk email that is sent with URL's, which when clicked leads to phishing websites or installs malware in your computer. Email bombarding is sending huge number of emails that results in the crashing of email address or server

- Data diddling – is unauthorised altering of data. The data input by the user is altered before it is processed by the computer providing a different output than expected

Types of Cybercrime

• Phishing – is the act by which the cybercriminals try to get the personal data of users. The aim of criminal will be to steal money or required data for creating financial loss

• Logic bombs – is an instruction in a computer program that triggers a malicious act. It is mostly introduced at banks and financial institutions for committing financial crimes.

• Denial of Service attack - more requests than what could be handled are bombarded

• Virus attacks - viruses are programs that affect the data on a computer, either by altering or deleting it. They attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network

• Trojan attacks – is an unauthorised programme that gains control over another's system passively by representing itself as an authorised programme. The most common form of installing a Trojan is through e-mail

• Thefts based on Internet time – these criminals gain access to the login ID and password and log in at the same time as the authorized person for Internet surfing

• Web jacking – here the hacker gains access and control over the website of another and mutilates or changes information on the site for political objectives or for a ransom

Prevention of Cybercrime

Widespread use of Internet has increased the connectivity, equally it has increased the thefts, fraudulent activities, and abuse. Adhering to proper security measures is the best defence against cybercrime. Following are a few security measures to adhere with:

• Protect your Computer: If your computer is not secured, it is prone to data theft for misuse. So install the necessary antivirus, firewall and anti-spyware and ensure they are running properly with latest version.

• Update Operating Systems: Ensure your applications and operating systems are updated with the latest available systems.

Prevention of Cybercrime

• Use Secure Wi-Fi: Check and modify the default settings in your personal Wi-Fi connection. Do not make any financial transactions in public Wi-Fi.

• Passwords: Create strong passwords for all your accounts and do not write them anywhere. Also change your passwords frequently.

• Emails: Be secured while sending financial or personal data in emails. Modify the privacy settings as needed.

• Protect your Mobile Devices: When you download applications ensure that it is a trusted source.

• Protect your Data: Encrypt important files with passwords and also take regular backups and store them in different location.

• In Social Media: Do not share private images or texts in the social media account because once it is in the Internet it is there forever. Also set the account as private.

• Browsing: While browsing be careful about the sites you visit. Avoid visiting sites by clicking url's provided in emails or blogs.

Threat to India's Economy in 2015

India has become a favourite place for the hackers. The study by an Assocham-Mahindra SSG has warned that the cybercrime rate in India might double to 300,000 (three hundred thousand) in 2015. As per the study's findings, total number of cybercrimes registered during 2011, 2012, 2013 and 2014 was at 13,301, 22,060, 71,780 and 1,49,254. The use of mobile phones and other devices to perform online financial transactions are increasing the risks. Many smart phones users do not perform a security check before downloading materials from the Internet. Performing online transactions using banking applications in mobile phones stores the user's details. When the mobile is hacked or stolen, the financial information is also stolen. The three major states contributing to 70 percent of India's revenue through Information Technology (IT) and the IT related industries are Andhra Pradesh, Karnataka and Maharashtra (Source: http://www.assocham.org/newsdetail.php?id=4821). These three States have registered the highest rate of cybercrimes under the new IT act in India, which can lead to the downfall of India's economy.

Conclusion

Human mind and conduct is immeasurable. Therefore, eliminating cybercrime from the cyber space is near to impossible. When one crime is investigated, a new one crops up. Nevertheless, it is definitely possible to curtail cybercrime. Criminals use their knowledge and expertise to be successful, and defenders must use the same approach to make them fail. Preventive measures cost less than the irreparable damages caused by cybercrime.

Reference

http://www.ukessays.com/essays/information-technology/mode-and-manners-of-committing-cyber-crime-information-technology-essay.php

https://sites.google.com/site/callingoffcybercrime/types-of-cyber-crime

http://utsavmtripathi.hubpages.com/hub/Types-of-cyber-crime-which-must-be-avoided

http://www.rrtd.nic.in/cyber_crime.htm

http://www.assocham.org/newsdetail.php?id=4821

About the Author

Mohammed Samiuddin spearheads the branding aspects & managing client relationships of ITMR. His passion includes speaking on cyber security threats, data security practices and new technological areas.

About ITMR

Institute of Technology, Management and Research (ITMR), a division of Mamta Trust, is a premier institute that provides world class professional training programs for the corporates and academic sector. ITMR's motto 'yogah karmasu kausalam' means 'Yoga is excellence in action' and is the foundation of its vision to evolve into a "CENTRE OF EMINENCE" to offer cutting edge vocational skills and mold professionals to become business and technical domain experts. ITMR's professional and corporate training programs include several cutting edge to help working professionals acquire domain expertise and meet the current and emerging challenges in the IT world.

Our flagship training program on Cyber security has (PDCIL) Professional Diploma in Cyber Investigations and Laws is a top of the class cyber security program in the country that trains top officials in the Police departments, Indian and International Banks, Military, Legal fraternity, Fortune 100 Global companies and Blue Chip India IT companies.

ITMR also offers research programs on Cyber Security (network security monitoring and access products), in association with Secure IQ, a leading provider of network security software products with headquarters in Fairfax, Virginia, USA and operations and development in Chennai, India.

Institute of Technology Management & Research
(Division of Mamta Trust)
2/850, Mugaliwakkam Road, Mugaliwakkam, Chennai - 600 125, Tamil Nadu, INDIA.
Admin Office: HTC Towers, No.41, GST Road, Guindy, Chennai – 600 032,
Tamil Nadu, INDIA. Phone: +91 44 4345 3500 / +91 44 4345 3349
Contact for More Information: training@htcitmr.ac.in