IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Cyber Crime and Its Preventive Measures

Manpreet Kaur[1], Gurinder Kaur [2], Er. C.K. Raina[3]

CSE Department, Adesh Institute of Technology, Gharuan, Punjab, India[1,2]

HOD, CSE Department, Adesh Institute of Technology, Gharuan, Punjab, India[3]

Abstract: Cybercrime is becoming ever more serious. Findings from the 2002 Computer Crime and Security Survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age. In this paper, we define different types of cybercrime and review previous research and current status of fighting cybercrime in different countries that rely on legal, organizational, and technological approaches. We focus on a case study of fighting cybercrime in India and discuss problems faced. Finally, we propose several recommendations to advance the work of fighting cybercrime.

Keywords: Cyber Crime, Cyber Security, Hacking, Phishing.

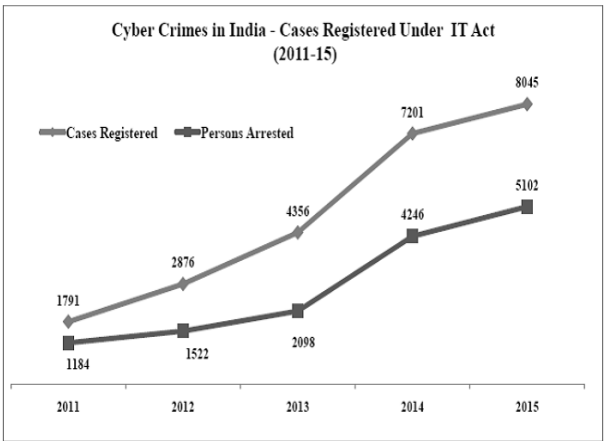
1. INTRODUCTION

Cybercrime is a crime in which a computer is used for the crime like hacking, spamming, phishing etc.
Cybercriminals use internet and computer technology to hack user's personal computers, smartphone data, personal details from social media, business secrets, national secrets etc. Criminals who perform these illegal activities through internet are called – Hackers. Though law enforcement agencies are trying to tackle this problem, it is growing regularly and many people have become victims of identity theft, hacking and malicious software. One of the best ways to stop this criminal and protecting any sensitive information is by making use of inscrutable security that uses a unified system of software and hardware to authenticate any information that is accessed over the Internet. Let's find out more about cybercrimes.

2. LITERATURE SURVEY

2.1. Cybercrime

Cybercrime is 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.



Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

2.2. Cyber security

Cyber security standards have been created recently because sensitive information is now frequently stored on computers that are attached to the internet. Also, many tasks that were once done by hand are carried out by computer; therefore, there is a need for Information Assurance and security. Cyber security is important to individuals because they need to guard against identity theft. Businesses also have a need for this security because they need to protect their trade secrets, proprietary information, and customer's personal information. The government also has the need to secure their information. This is particularly critical since some terrorism acts are organized and facilitated by using the internet.

2.3. Causes of Cyber Crime

The reasons for the vulnerability of computers may be said to be:

- **Easy to access** – The problem behind safeguarding a computer system from unauthorized access is that there are many possibilities of breach due to the complex technology. Hackers can steal access codes, retina images, advanced voice recorders etc. that can fool biometric systems easily and bypass firewalls can be utilized to get past many security systems.
- **Capacity to store data in comparatively small space** – The computer has unique characteristic of storing data in a very small space. This makes it lot easier for the people to steal data from any other storage and use it for own profit.
- **Passion of youngsters:** Cybercrimes can be committed for the sake of recognition. This is basically committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

They do not mean to hurt anyone in particular; they fall into the category of the Idealists; who just want to be in spotlight.

- **Desire of Making quick money:** Another cause of cyber-crime is to make quick money. This group is greed motivated and is career criminals, who tamper with data on the net or system especially, e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers.
- **Misconception of fighting a Just cause:** This is the most dangerous of all the causes of cyber-crime. Those involve believe that they are fighting a just cause and so do not mind who or what they destroy in their quest to get their goals achieved. These are the cyber-terrorists.
- **Complex** – The computers run on operating systems and these operating systems are programmed of millions of codes. Human mind is imperfect, so they can do mistake at any stage. The cyber criminals take advantage of these gaps.
- **Negligence** – Negligence is one of the characteristics in human conduct. So, there may be a possibility that protecting the computer system we may make any negligence which provides a cyber-criminal the access and control over the computer system.
- **Loss of evidence** – The data related to the crime can easily destroyed. So, Loss of evidence has become a very common & obvious problem which paralyses the system behind the investigation of cyber-crime.
- **Accessibility to Victims:** The amount of people online allows criminals to target their victims without being physically present. Police find it impossible to implicate people when the trail is online.
- **Inaccessibility to Criminals:** By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and even bypass firewalls can also be utilized to get past many a security system. Though technology is improving there is a long way to go before cyber criminals can be policed vigilantly.
- **Loopholes in system:** There are always loopholes in security that a professional cybercriminal can find and hack into. The traditional bank robber researched the security system and took advantage of it; a cyber thief is not much different, except he can breach security virtually.

2.4. Cyber Criminals:

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind.

The following are the category of cyber criminals-

a) Children and adolescents between the age group of 6 – 18 years:

The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other reason may be to prove them to be outstanding amongst other children in their group. Further the reasons may be psychological even.

b) Organized hackers:

These kinds of hackers are mostly organized together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. Further the NASA as well as the Microsoft sites is always under attack by the hackers.

c) Professional hackers / crackers:

Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

d) Discontented employees:

This group includes those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

2.5. Types of Cybercrimes

Against Individuals: –
I. Pestering via e-mails.
ii. Cyber-stalking.
iii. Distribution of obscene material.
iv. Insult.
v. Illegal control over computer system.
vi. Offensive exposure
vii. Email spoofing
viii. Cheating & Fraud

Against Individual Property: -
i. Computer vandalism.
ii. Transmitting virus.
iv. Unofficial access over computer system.
v. Logical Property crimes
vi. 'Internet time' thefts

Against Private Organization: -
i. Unauthorized control/access over computer system
ii. Ownership of non-permitted information.
iii. Distribution of pirated software etc.

Against government/nation: -
i. Cyber terrorism against the government organization.

Against Society at large: -
i. Pornography (basically child pornography).
ii. Polluting the youth through coarse exposure.
iii. Trafficking
iv. Monetary crimes
v. Sale of illegal articles
vi. Online betting/gambling
vii. Forgery

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

2.6. The Modes & mannerism of committing crime

a) **Computer viruses: Viruses** are programs that affix themselves to a computer or a file and then flow themselves to other files and also to other computers on a network. They typically influence the data on a computer, either by changing or deleting it.
Worms on the other hand do not interfere with data. They simply multiply until they fill all available space on the computer.
b) **Malware:** Also**,** known as malicious software. It's a software that is used to achieve awful things by corrupting peoples' private data. It steals data like passwords, etc. and sends them to the creator of malware and these data are used by him to threaten or steal computer based items for personal use.
c) **Trojan Attacks:** Trojan attacks occur from Trojan Horse. A Trojan Horse is an unauthorized program which gains control over another system by presenting itself as an authorized program. Most of them come through e-mails.
d) **The Salami Attacks:** It is used to commit financial crimes. In this type of crime small alterations are done by people on transactions to gain money without getting noticed.
e) **Email Bombing:** It is sending a large number of junk or useless mails to a person or a company which leads to crashing of the computers.
f) **E-mail Spoofing:** It is changing the email header and other parts of the sender's address to make it appear as it is from another location or source.
g) **Web Jacking**: In this type of crime a hacker gains access and control over a website and alters, changes or deletes information on the website.
h) **Logic Bombs:** These are programs similar to real bombs which have a trigger. These are used to threaten companies for gaining money. They completely delete everything present on the computer system on which they act on. Once triggered, nothing can stop them. They are also called event dependent programs.
i) **Data Diddling:** It is a kind of attack which involves altering data before it is processed by the computer so that incorrect results are obtained.
j) **Denial or Distributed denial of Service Attack:** In this type of crime the victim's computer is overloaded with requests than it can handle leading the computer system to crash. In distributed denial of service attack the perpetrators are more than one and far away from each other. It is very difficult to control such attacks.
k) **Intellectual property crime:** This crime includes unauthorized copying and distribution of original software. Pirating of games, movies etc. are examples.

2.7. Consequences of Crime

1. Loss of Revenue:
One of the main consequences of cybercrime on a company is a loss of revenue/income. This loss may be caused by an outside person who acquires sensitive financial information, using it to extract funds from an organization. It can also come about when a business's e-commerce site becomes compromised--while terminal, expensive income is lost when consumers are unable to utilize the site.

2. Wasted Time:
Another major consequence of cybercrime is the time that is wasted when Information Technology personnel must dedicate maximum part of their day handling such incidences. Rather than working on productive and creative measures for an organization, many Information

3. Damaged Reputations:
In situations where customer records are compromised by a security contravene associated with cybercrime, a company's reputation can take a major batter.

4. Influence of Cyber Terrorism:
Cyber-terrorism can have a serious large-scale influence on significant numbers of people. It can weaken countries' economy greatly, thereby stripping they're of its resources and making it more vulnerable to military attack. Cyber-terror also affects internet-based businesses. Like brick and mortar retailers and service providers, most websites that produce income (whether by advertising, monetary exchange for goods or paid services) could stand to lose money in the event of downtime created by cyber criminals.

5. Impact on Government and Society:
Cybercrime has been increasing its convolution and financial expenses since corporations have begun to use computers in the course of doing business. As technology increases between governments that are caught up in international business, criminals have realized that this is a cost-efficient method of making money. This investigation and testing manual is meant to provide as a basic model on the lessons learned to set up governments, and their prosecutors, for combating cybercrime. To research deeply into computer technology requires both long learning and technical expertise. Therefore, as in most of the crimes that are technological in nature, or have technical aspects to them, such as bank hoax or murder investigations that necessitate the analysis of blood and spatter techniques, gun-shots that require extensive ballistics investigation, experts are advisable for use as an aid in directing your investigations, to act as a special aide in preparing for trial, and as an expert to testify in that trial.

1. The provisions of the I.T. Act have no application to negotiable instruments, power of attorney, trust, will and any contract for sale or conveyance of immovable property.
2. The Act applies to any cyber offence or contravention committed outside India by a person irrespective of his/her nationality.
3. As provided under Section 90 of the Act, the State Government may, by notification in 'Official Gazette' make rules to carry out the provisions of the Act.
4. Consequent to the passing of this Act, the SEBI had announced that trading of securities on the internet will be valid in India, but initially there was no specific provision for protection of confidentiality and net trading. This lacuna has been removed by the IT (Amendment) Act, 2008.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

3. PREVENTIVE MEASURES

3.1. How to Tackle Cyber crime

To tackle cybercrime effectively, establish multidimensional public-private collaborations between law enforcement agencies, the information technology industry, information security organizations, internet companies and financial institutions. Unlike the real world, Cyber criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals.

- **Use Strong Passwords:** Use different password and username combinations for different accounts and resist the temptation to write them down.
- **Be social media savvy:** Be sure to keep your social networking profiles (Facebook, Twitter, YouTube, etc.) are set to private. Be sure to check your security settings. Be careful of what information you post online. Once it is on the Internet it is there forever.
- **Secure your Mobile Devices:** Many people are not aware that their mobile devices are also vulnerable to malicious software, such as computer viruses and hackers. Be sure to download applications only from trusted sources. It is also crucial that you keep your operating system up-to-date.
- Be sure to install anti-virus software as well. Be sure to use a secure lock screen as well. Otherwise, anyone can access all your personal information on your phone if you misplace it or even set it down for a few moments. Someone could even install malicious software that could track your every movement through your GPS.
- **Protect your data:** Protect your data by using encryption for your most sensitive files such financial records and tax returns.
- **Protect your identity online:** When it comes to protecting your identity online it is better to be too cautious than not cautious enough. It is critical that you be cautious when giving out personal ID such as your name, address, phone number and/or financial information on the Internet. Be certain to make sure websites are secure when making online purchases, etc. This includes enabling your privacy settings when using/accessing social networking sites.
- **Keep your computer current with the latest patches and updates:** One of the best ways to keep attackers away from your computer is to apply patches and other software fixes when they become available. By regularly updating your computer, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system.
- **Parental control:**
  Monitor the online activities of your children. They should only have access to a computer located in a central area of your home and you should regularly check all browser and email activity. A wise thing to do is to use parental control software that limits the types of sites the user can gain access to.
- **Avoid Spyware/Ad-ware:**
  Spyware and ad-ware take up the memory and can slow down the computer or lead to other problems. Use Ad-Aware and Spy-bot to remove spyware/ad-ware from the computer. Be cautious of invitations to download software from unknown internet sources
- **Back Up Important Files:**
  Reduce risk of losing files to a virus, computer collapse, robbery or tragedy by producing back-up copies. Keep your critical files in one place on your computer's hard drive so you can easily create a backup copy. Also, Save copies of files to a CD, online, or USB drive. Store your back-up media in a secure place away from the computer, lest of robbery or fire. Test the back-up media occasionally to verify if the files are readable.
- **Call the right person for help:** Try not to panic if you are a victim, encounter illegal online content, such as child exploitation, or if you suspect a cyber-crime, identity theft or a commercial scam. Just like any other crime report this to your local police.

3.2. DETECTION

Regrettably, there is no cut-and-dried way for detecting cyber-crime. Today, a large number of cybercrimes are detected by chance. However, recent experience has shown some more or less informal methods by which an individual can detect cyber-crime.

1. Reviewing:

Audit the system frequently. Be attentive to any irregularities in the system. As of now, it is generally the uncertainties of employees or managers that lead to the capturing of a perpetrator. Most of the computer crimes do not draw from distant "hackers," but normally comes from employees or people the operator knows. Most computer crimes are done by employees working on large network systems in organizations managing a lot of computerized cash. Apparently, banks, large firms, government offices and universities are susceptible, and, known the size of the organizations, it can take months to detect with any certainty.

2. Checking mistakes:

Check for mistakes. Many authorities claim that cyber criminals can get too gluttonous and begin to get careless. Employees who are aware of this crime often get nervous and turn the perpetrator in. These similarities have been seen to happen with family members of the cyber-criminal too. The probability of this working is greater if employees know clearly that cyber-crime will result in full prosecution.

3. Email inspection:

Some types of cybercrime, such as cyber-stalking or cyber defamation, are carried out by email and can be detected and tracked by investigating the email header. The email header is info that travels with every mail, including the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Internet Protocol (IP) address of the dispatcher and the date and time at which the message was sent. Using this information, law enforcement agency officials get hold of the address and telephone number of the sender from the internet service provider.

4. Using government:

Make full use of government agencies to help detect cybercrime. It happens frequently that audits by the IRS or investigations by police turn up the continuation of cybercrime that had gone undetected for a long while. Things like inventory shortages and abnormalities in the allotment of income within the organization can be signals that crime is being committed over the network. Nonetheless, it is generally hunches that reveal computer crime, when it is detected.

3.3. TECHNOLOGIES TO CURB CYBER ATTACKS

In order to stay ahead and protect their data and businesses, security teams must adapt fast in the escalating arms race. Security and risk leaders need to fully engage with the latest technology trends if they are to define, achieve and maintain effective security and risk management programs that simultaneously enable digital business opportunities and manage risk

To help them, analyst firm Gartner has unveiled its top ten technologies that organisations must have in their arsenal: -

1) **Cloud access security brokers: -** Cloud access security brokers (CASB) provide data security professionals with a critical control point for the secure and compliant use of cloud services across multiple cloud providers.
2) **Endpoint detection and response (EDR): -** EDR tools typically record numerous endpoint and network events, and store this information either locally on the endpoint or in a centralised database. Databases of known indicators of compromise. Behaviour analytics and machine-learning techniques are then used to continuously search the data for the early identification of breaches, including insider threats, and to rapidly respond to those attacks.
3) **Non-signature approaches for endpoint prevention**: - Purely signature-based approaches for malware prevention are ineffective against advanced and targeted attacks.
   Multiple techniques are emerging that augment traditional signature-based approaches, including memory protection and exploit prevention that prevent the common ways that malware gets onto systems, and machine learning-based malware prevention using mathematical models as an alternative to signatures for malware identification and blocking.
4) **User and entity behavioural analytics: -** User and entity behavioural analytics (UEBA) enables broad-scope security analytics, much like security information and event management (SIEM) enables broad-scope security monitoring. UEBA provides user-centric analytics around user behaviour, but also around other entities such as endpoints, networks and applications. The correlation of the analyses across various entities makes the analytics' results more accurate and threat detection more effective.
5) **Remote browser: -** Most attacks start by targeting end-users with malware delivered via email, URLs or malicious web sites. An emerging approach to address this risk is to remotely present the browser session from a 'browser server' (typically Linux based) running on-premises or delivered as a cloud-based service.
   By isolating the browsing function from the rest of the endpoint and corporate network, malware is kept off of the end-user's system and the company has significantly reduced the surface area for attack by shifting the risk of attack to the server sessions, which can be reset to a known good state on every new browsing session, tab opened or URL accessed.
6) **Deception: -** Deception technologies are defined by the use of deceits and/or tricks designed to thwart, or throw off, an attacker's cognitive processes, disrupt an attacker's automation tools, delay an attacker's activities or disrupt breach progression. For example, deception capabilities create fake vulnerabilities, systems, shares and cookies.
7) **Block chain tech.** Block chain isn't a term familiar to many, but it's associated with a technology that most have heard of—Bitcoin. Block chain is a system of collaborative information storage, exchange, and retrieval that maintains a public record of ownership. It's how Bitcoin transactions are able to take place, and remain consistent, without any single institution defining or monitoring those transactions, and without any outside interference to commit digital theft. Shaping Tomorrow predicts that within a few years, most major banks (as well as other financial-related companies like insurance institutions) will be using block chain to greater secure their financial transactions.
8) **Biometrics: -** In the public eye for decades, biometric technology uses unique personal identifiers to ensure proper identification. For example, your phone may take a thumbprint scan before allowing you to access the data inside, or a device may scan your retina before permitting you access to a building. Since these personal identifiers are incredibly hard to mimic, especially remotely, they could greatly enhance security in a number of different areas. However, there are still a number of important hurdles to overcome before the technology can be adopted on any wide scale.

4. CONCLUSION

Capacity of human mind is unfathomable. It is not possible to eliminate cybercrime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime. Undoubtedly the Act is a historical step in the cyber world. Further I all together do not deny that there is a need to bring changes in the Information Technology Act to make it more effective to combat cybercrime. I would conclude with a word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive.

REFERENCES

[1] https://sites.google.com/site/callingoffcybercrime/
[2] Dr.B.Muthukumaran "**CYBER CRIME SCENARIO IN INDIA"**
[3] http://www.cyberlawsindia.net/
[4]https://www.ieee.org/publications_standards/.../2014_04_msw_a4_format.doc
[5]https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/
[6]http://www.information-age.com/gartner-picks-out
[7] http://a4academics.com
[8] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
[9]Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, 2010.
[10]Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, ISBN 0-471-38922-6
[11]Morrie Gasser: Building a secure computer system ISBN 0-442-23022-2 1988
[12]Stephen Haag, Maeve Cummings, Donald McCubbrey, Alain Pinsonneault, Richard Donovan: Management Information Systems for the information age, ISBN 0-07-091120-7
[13]E. Stewart Lee: Essays about Computer Security Cambridge, 1999
[14]Peter G. Neumann: Principled Assuredly Trustworthy Composable Architectures 2004
[15]Paul A. Karger, Roger R. Schell:
[16]Thirty Years Later: Lessons from the Multics Security Evaluation, IBM white paper.
[17]Bruce Schneier: Secrets & Lies: Digital Security in a Networked World, ISBN 0-471-25311-1
[18]Robert C. Seacord: Secure Coding in C and C++. Addison Wesley, September, 2005. ISBN 0-321-33572-4