CONCEPTUAL RESEARCH PAPER

COMPUTING TRENDZ Vol VII No. 1,2 , January - December 2017 Print ISSN : 2230-9152, Online ISSN 2456-138X

# Issues Related with Cyber Crime and Security

Poorva Sanjay Sabnis
Assistant Professor, Department of Computer Science, School of Management Sciences, Varanasi

**ABSTRACT**
This paper mainly focuses on the current world-wide problem of cyber crime and its related security. We can define cyber crime as the crime related with the information available on the internet..!! Here main objective is to hack the data from various computers and misuse that confidential data. Basically there are two types of data hacking : active and passive. In active hacking, we can realized that our data is hacked and being misused. But in case of passive attack, hacker is silently observing our data and use this information for other purposes. Since we can not realizing that our data is being hacked, its more dangerous. In case of cyber security also, these two types of attackes are included. Cyber security is related with the information security on the internet. Cyber crime is the serious issue, we have to find the nature of attack and solutions required for that attack. Cyber security plays an important role in the development of information technology as well as internet services because internet services allows us to access huge amount of information such as data, texts, images, videos, graphics, softwares from the internet.

**Keywords :** Cyber security, cyber crime, attacks, hacking
*Computing Trendz (2017*). DOI: 10.21844/cttjetit.v7i1-2.1

## Introduction

We can define cyber security as complete package of technologies, processes and practices mainly designes for protecting computers, networks, softwares and data from attackes ( may be active or passive ), and unauthorized use. Because cyber crime mainly focuses on the confidential data available on the internet. Cyber crime can be defined as any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. The commonly accepted definition of cyber security is the protection of any computer system, software program, and data against unauthorized use, disclosure, transfer, modification, or destruction, whether accidental or intentional.

If people want to protect there computers, networks, softwares and data, they should take care while making set-up, maintain and use of computers and the mainly, the Internet. Cyber-security includes overall physical protection (both hardware and software) of personal information and technology resources from unauthorized access. The problem of cyber secrity can be solved with a joint partenship between IT community and general people.

The seriousness of cyber crime is even greater if it affects critical IT systems of telecommunications, power distribution, banking or transport, i.e. of the infrastructure on which virtually all individual companies depend. Cyber crimes are rapidly growing because of the rapidly growing

**Corresponding Author:** Poorva Sanjay Sabnis, Assistant Professor, Department of Computer Science, School of Management Sciences, Varanasi, e-mail: poorva@smsvaranasi.com
**How to cite this article:** Sabnis, P.S. (2017). Issues Related with Cyber Crime and Security. Computing Trendz 7(1&2): 1-5
**Source of support:** Nil
**Conflict of interest:** None

interconnectivity between IT systems, via Intra-nets, Extra-nets and the Internet itself, as well as by direct physical interconnection, or exchangeable storage media such as pendrives. Also we have make alertness in the people about various attacks and remedies on the cyber security.

**Cyber security and cyber crime**

Cybercrime and cyber security are interrelated issues that can notbe separated in an interconnected environment. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services.

Cyber Security is the process and it involves techniques related with protecting sensitive data, computer systems, networks and software applications from cyber attacks. The cyber attacks are general terminology which covers a large number of topics, but some of the popular are:

- Tampering systems and data stored within.
- Exploitation of resources
- Unauthorized access to the targeted system and accessing sensitive information
- Disrupting normal functioning of the business and its processes
- Using ransomware attacks to encrypt data and extort money from victims

The attacks are now becoming more innovative and sophisticated that is capable of disrupting the security and hacking the systems. So it's very challenging for every business and security analyst to overcome this challenge and fight back with these attacks.

To understand the need for Cyber Security measures and its practices, let's have a quick look at the types of threats and attacks.

**Threats to Cyber Security :**

A threat can be defined as a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm according to the computer security. Threats to cyber security can be roughly divided into two general categories:

1) Threats related with the actions having aim of damage or destroy cyber systems

2) Threats related with the actions that seek to exploit the cyber infrastructure for harmful purposes without damaging or compromising that infrastructure. It is called as cyber exploitation. While some intrusions may not result in an immediate impact on the operation of a cyber systems, as for example when a Trojan Horse infiltrates and establishes itself in a computer, such intrusions are considered cyber attacks when they can thereafter permit actions that destroy or degrade the computer's capacities.

Cyber exploitation includes using the Internet and other cyber systems to commit fraud, to steal,to recruit and train terrorists, to violate copyright and other rules limiting distribution of information, to convey controversial messages (including political and - hatel speech), and banned materials. Following are some new threats to cyberspace. With the proliferation of free hacking tools and cheap electronic devices such as key loggers and RF Scanners, if you use e-mail or your threat can be defined as a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm according to the computer security.

### How we can development the software tools that automate the attacks :

Now-a-days, there are so many software tools which are going to use for automate attack. In the automate attack, some procedures for attack are pre-installed in the software. Using this software and pre-installed attack, a single man, we can say hacker, can attack attack thousands of a computer systems in a single day with the help of single computer. This integrity may extend to multiple computers too. Since most of these software tools use preset methods of attacks, not all attacks prove successful. There is one of the best solution for any user that, the users who update their operating systems and software applications on a regular basis reduce their risk of attacks. Because the companies who are developing protection software analyse attack tools and prepare for the standardized hacking attacks. High-profile attacks are often based on individually-designed attacks.

### Mobile Devices and Apps :

Currently, there is wide growth of mobile devices which are also facing the same problem of security. Here risk factor is high related with hacking of the data. Every new smart phone, tablet or other mobile device, when opens another window for a cyber attack as each creates another vulnerable access point to networks. This dynamic activity is no more secret to the hackers. They are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the another important problem is of losting and stolling the devices. It gives another chance to include these new technologies and old ones that previously flew under the radar of cyber security planning.

### Social Media Networking :

Another, the most important aspect of cyber security is related with rapidly increasing use of social media networking sites such as facebook, whatsapp, LinkedIn etc. A social networking site is an online platform that allows users to create a public profile and interact with other users on the website. Social networking sites usually have a new user input a list of people with whom they share a connection and then allow the people on the list to confirm or deny the connection. Because of high demand of social networking sites, there is fear of personal cyber threats. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

### Cloud Computing :

Currently, more companies uses cloud computing. The use of cloud computin is highest because it saves the cost and efficient in use. For using the cloud computing, there is need of a well designed architecture and operational security planning. It will help organizations to effectively manage the risks of cloud computing. But unfortunately, current surveys and reports indicate that companies which understand the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

### Necessity of Cyber Security :

In the recent days, information is the most valuable aspect with respect to an individual, companies, state and country too.

Following are the some concerned areas :

- We have to protect unauthorized access, disclosure, modification of the resources of the system.
- There should be security during e-coomerce ( on-line cash payment transactions) regarding shopping,banking, railway reservations and share markets.
- There must be security of accounts while using social-networking sites . It will helps to reduce the risk of hacking.
- The most important key is for improving the cyber security is a better understanding of the various threats and attacks used by the attacker.
- There is need of separate unit to handle security issues of the organization.
- In the different organizations or missions, there may be different types of adversaries, with different goals, and thus need different levels of preparation.
- We have to secure the information containing various essential surveys and their reports.

**Security Training and Awareness :**

It is truly said that, the human is the weak entity in any information security program.

Communicating the importance of information security and promoting safe computing are key in securing a company against cyber crime. Following are the some guidelined :

- Use a password having combination of upper and lower case letters, numbers, and symbols to make it less susceptible to brute force attacks.
- Do not share or write down any password.
- Communicate/educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets.
- Do not click on links or attachments in e-mail from untrusted sources.
- Do not send sensitive business files to personal email addresses.
- Have suspicious/malicious activity reported to security personnel immediately. Secure all mobile devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation.
- Educate employees about phishing attacks and how to report fraudulent activity.
- Do not share any bank details, OTP with anyone. Also do not share ATM number.

**CONCLUSION :**

This paper mainly focuses on cyber crime and security realted issues. It also focuses on types of attacks which may happen on the data. It also gives a brief idea about cyber crime and cyber security i.e how cyber crime may occur and which care should be taken by every indivisual either at personal level or at corporate level. This paper also focuses on the various threats to Cyber Security. It also gives the idea about the automated attacks using pre-installed software. There is brief idea about the necessacity of the cyber security in todays era. It also gives some idea about socail awareness about cyber security and cyber crime.

**References :**

Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/103537.pdf

http://userpage.fuberlin.de/~jmueller/its/conf/Madrid02/abstracts/GhernaoutiHelie.pdf

www.met.police.uk/pceu/documents/ACPOecrimestrategy.pdf

Guinier D, Dispositif de gestion de continuité – PRA/PCA: une obligation légale pour certainset un impératif pour tous (Continuity Planning – BRP/BCP: a legal requirement for some and a vital necessity for all). Expertises, no. 308, Nov. 2006, pp. 390 -396.