Cyber Security: Issues & Challenges

Dr. Subhash Kumar

The phenomenal growth in the field of technology has changed our life and the dependency on technology has increased immensely. Internet has become the real mode of fulfilling all the needs. As the technology is evolving and growing, numerous types of cyber crimes are also rising immensely on a regular basis throughout the world. This trend has posed many challenges to the security at all levels and safeguarding the information has been one of the biggest challenges of modern time. ***cyber security*** is a matter for concern for everybody today The Internet has become an essential infrastructure for both businesses and individual users and its security has therefore become a priority issue.Attaining and sustaining a safe cyberspace is a complex procedure, and the major worries include individual identity, privacy, safety, intellectual property. The dangers to a protected and effective structure are severe like cybercrime, cyber war, cyber espionage and cyber terrorism. An alertness and fundamental understanding of the risks posed in a cyber-world will help in protectingthe digital assets and intellectual property along with the business. Hence, this paper is an attempt to classify threat types and various challenges faced by cyber security on the most recent technologies.It also aims on the cyber security methods, and the trends of cyber safety measures.

In modern times, society operates largely on technology and dependency on technology is increasing day-by-day for each and everything.Technology has its limitations and along with the paramount facilities it also brings serious threats also.With the wide scope that it provides, it also turn out to be a central point for cybercrime and cyberattacks. So, safeguarding it is extremely important.Now a days most of theneeds depend on internet, and people use it for social connections and education.The Internet is useful in making national and international expansion and creates an environment for various groups to successfully perform collectively through lowered storing and communication expenses which helps the authority to provide useful help to constituents. Besides, the Internet is also important as internet generally may give overall service on sizable range of subjects in a limited time while earlier it used to take lot of time for the same results.

As far as the term cyber is concerned, it is important to understand that from a security point of view, the term “cyber” normally means anything related to information technology. It generallymeans the usage of electronics to connect between objects. It comprises the Internet as the vital data conveyance component but can also incorporate other technical devices. Cyber encourages the business, learning, administrative, and important national infrastructure. It is also true that the services are prevalent and expand beyond domestic borders, people, organizations, and it can be used for constructive and destructive purposes. Cybersecurity is not a simple issue and it includes many electronics devices and aspects. Cyberspace is a virtual world formed by computer, desktops, and mobile phones,broadband and wireless signals that helps the educational institutions, corporates, health facilities, government, and individual lives through an advanced set of communication systems, accessible globally. (Obama, 2009).

Cyberspace is generally described the interconnectedsystem (network) that is technology deals in information,telecommunication, tele-businesses and in cooperate world incorporates with the help of Internet processors and controllers in important businesses (The White House, 2008). Cyberspace is usually considered as method or program concerning,”to the usage of the Internet for data handling transmission or usage in telecommunication”.All over the world Cyberspace is influential in nourishing the dailyhappenings of masses and organizations.throughout the world.

Cyber Crime

With the growing technology, cybercrime has also become a major threat to the society. Various forms of cybercrime are a causing multiple problem at all levels starting from individual to the nations. The basic understanding of Cybercrime is used for any illegal activity that operates a computer as its key means of commission and theft. In fact, when computers are used to take secret information, then it is known as cybercrime, generally for financial gain. Cybercrime is reflected in a various form such as attacks on websites with the help of technology by the hacker, to gain monetary value through unlawful and unethical procedures. The technology develops a lot of tools to make these businesses success, these devices compriseof change in physical device, ransomware, spyware,malware and social engineering. There can be following four types of cyber-attacks: cyber terrorism, cyber war, cybercrime, and cyber espionage.(Shackelford, 2012): Some definitions are mentioned below (Lord & Sharp, 2011)

Cyber espionage:The usage of computers to collect intelligence.

Cyber terrorism: The usage of computers or allied systems to establish fear in any society and leads to destruction as well.

Cyber war: The army operations executed within cyberspace in order to refute an enmity, whether a nation or nonstate person, to achieve a political end.

Types of Cyber Crimes

Identity theft –It is primary related to the theft of personal financial resources. This is done with a purpose of stealing financial resources of a person.

Cyberterrorism –It is very serious cybercrime which involves not persons, organizations but also the nations. Normally, it involves computer technology thatdeliberate attack on theCorporate and Governmentbusiness.

Cyberbullying – It is when an adolescent harasses or defames someone through internet, or any other medium of technical devices or any other social network then, it is known as Cyberbullying. The same crime is known as Cyberstalking, if performed by adults,

Hacking –It is extremely widespread cybercrime where; someone gets entry to other'sdevices and for the usage of passwords for unfair benefit.

Defamation – If anyone's statement on internet platforms causes harm to the reputation of any individual or organization.

Copyright - Any usage of someone's copyrighted without his/herconsent is a punishable crime.

Trade Secrets – 'Generally Internet organizationsused to spend plenty of time and money in improving software, applications. Hence, they depend on C0yberlaws to safeguard their data along with their business secrets against burglary.

Freedom of Speech – It is important to understand,"thatthere is a very narrow line between freedom of speech and being a cyber-offender. As freedom of speech enables individuals to speak their mind, cyber law refrains obscenity and crassness over the web".

Harassment and Stalking – It is illegal at internet platforms. It is important to note that Cyberlaws safeguard the sufferers and act against the offender in such case.

Risky Areas in the Cyberspace Domain Major Security Threats

• Business • Industrial aspects • Safety related issues • Intellectual property related issues • Technological aspects • Cultural aspects • Policy related issues • Diplomatic issues	• Issues related to Virus • Worm related threats • Trojan horse • Spyware related threats • Spam issues • Hoax issues • Adware issues • Rootkit related issues

Cyber Laws in India

In India there is provisions for cyber law or cybersecurity laws under "the Information Technology Act, 2000 or IT Act, 2000". There was a need for checks on IT related activities; hence, the prominence was on the forming of cyber laws. Thus, "the Information Technology Act, 2000, or also recognized as the ***Indian Cyber Act*** was formulated which is the main law in India dealing with cybercrime and electronic commerce". One of the major features of IT Act 2000 is thatthe Act also highlights on key issues of security, which are considered very important for the completion of electronic transactions. In India, the Internet Lawsendorses digital signatures andacknowledged the documents generated by means of digital signatures.

(file:///C:/Users/subhashk/Downloads/9745-Article%20Text-36208-1-10-20160621.pdf)

In India, the original IT Act 2000 had 94 sections, divided in 13 chapters and 4 schedules. It is important to note that the law is applied in the entire country."The act also defines cybercrimes and recommended penalties for them. It also formed a Cyber Appellate Tribunal for resolving disputes arise from this new law. The Act also amended various sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934 to make them compliant with new technologies".Besides, persons of various nationalities may also be accused according to the law if crime includes a computer or Internet link computernetwork.

There were some amendments in IT Act, 2000 in 2008 to tackle new challenges. These were made considering laws on cybercrime - IT Act, 2000 by way of the IT Act, 2008 which were implemented at the starting of 2009 to improve the cybersecurity laws as below.

- the existing usage
- authenticating the digitalsignature
- making the IP address holder accountable
- enforcing responsibility for data violations.
- Preventing Cybercrime

The efforts made through the IT Act 2000 & 2008 to combat the menace of cybercrime.But looking at the increasing role of internet in our life, it is always better to take following corrective and preventive measuresalong with the other efforts to minimize the risk of the cybercrime:

Unwanted message –Generally one used to receive text messages from an unidentified number. We should be very careful. We also need to stay away from replying to it.

Use of trustworthy Source for downloading –We should develop the habit of downloading everything on our devices from a reliable source only.

Avoid Providing the Private Information Invite – We might have experienced during receiving a call or mail where, the caller requests for individual information which involves card CVV or an mail including an attachment and it is desired there to click on inserted links. We need to avoid replying to any emails or calls like this.

Dealing with the Ransomware: It is to be understood that usually ransomware is delivered through malicious emails andfollowing important measures may be taken for protection:a) Staff awareness b)Installation and maintenance of decent anti-virus and malware protection software. c)Updating the Software on a regular basis.d)Need to keep the Data backups which willhelp to recuperate from an unencrypted version of a file.

Phishing: Phishing is an effort to get confidential information during masquerading as a trustworthy contact. Such emails may look completely convincing. The following steps may be taken for protection in this regard: a) always remember that such information are never asked by the companies.b)Always use anti-malware software. c)Turn on the spam filters.

Hacking: The following ways can be adopted to avoid hacking: a)Network firewalls can be used, b) data retrieve security, processes for delivering and removing access, and user recognition and training.

As discussed above in every sections, it is important to keep in mind that along with technology, sound equipped methods, techniques and consistent staff coaching may be extremely vital in safeguarding the valuable data.

Suggestions and Recommendations:

- People need to be trained on the multiple aspects of cybercrime because there is lack of awareness about cyber security act (IT Act 2000 & IT Amendment Act 2008) among the common people. So, many times when they face a cybercrime, they do not go for lodging a complaint.

- There is lack of clarity and overlapping between some of the Acts of IT Act 2000 (Section 43 & Section 66) and IPC 1860 (IPC Section 463,464, 468 and 469), which results in the delaying of the resolution.

- The digital literacy of rate of India is almost no-existent among more than 90% of India's population. Therefore, most of the population of India is not benefited from the Cyber Security Act. Govt and other agencies should focus on digital literacy for everyone in the country so as to minimise the risk of cyber related crimes.

References :

Cavelty, M., (2011) Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture, IP – Global Edition, ETH Zurich.
Conway, M. (2007). Terrorism and Internet Governance: Core Issues, Dublin: Disarmament Forum 3.
Davidson, M. (2009, March 10). The Monroe Doctrine in Cyberspace, Testimony given to the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Technology. Katzan, H., (2008). Foundations of Service Science: A Pragmatic Approach, New York: iUniverse, Inc.
file:///C:/Users/subhashk/Downloads/9745-Article%20Text-36208-1-10-20160621.pdf
Ramdinmawii Esther, Ghisingh Seema, Sharma Usha Mary: "A Study on the Cyber-Crime and Cyber Criminals: A Global Problem", International Journal of Web Technology,Volume: 03, June 2014, Pages: 172-179.
Saini Hemraj, Rao Yerra Shankar, Panda T.C. "Cyber-Crimes and their Impacts: A Review". International Journal of Engineering Research and Applications, Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209.
SarmahAnimesh, SarmahRoshmi andBaruah Amlan Jyoti, "A brief study on Cyber Crime and Cyber Law's of India". International Journal of Engineering Research and Applications, Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209.Vol. 04, Issue- 06, June -2017, pp.1633-1641.
Jain Neelesh, Shrivastava Vibhash,"Cyber Crime Changing Everything – An Empirical Study". International Journal of Computer Application. Issue 4, Volume 1, February 2014, pp.76.

**(Dr. Subhash Kumar, Associate Professor,
Department of Journalism & Mass
Communication, Jaipur)**