ISSN 2229-3531 (Print)
JUCIT Vol. 8(5), 30-36 (2017). Periodicity-2-Monthly
ISSN 2455-9997 (Online)

JOURNAL OF COMPUTER & INFORMATION TECHNOLOGY
An International Open Free Access Peer Reviewed Research Journal of Computer Science Engineering & Information Technology
website:- www.compitjournal.org
Estd. 2010

A Literature Review on Cyber Security in Indian Context

SHWETA GHATE and PRAGYESH KUMAR AGRAWAL*

Department of Computer Science, Institute for Excellence in Higher Education, Bhopal, M.P. (India)
e-mail: gh.shweta@gmail.com
*Department of Physics and Electronics, Institute for Excellence in Higher Education, Bhopal, M.P. (India)
Email of Corresponding Author e-mail: dr_p_agrawal@hotmail.com

http://dx.doi.org/10.22147/jucit/080501

Acceptance Date 04th October, 2017, Online Publication Date 20th October, 2017

Abstract

Cyber security comprises of technologies, processes and practices designed to protect computers, programs, networks and data from hacking, damage or unauthorized access. Cyber security is also sometimes conflated inappropriately in public discussion with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. Cyber security comes into picture as well as we encounter cyber crimes. To avoid giving cybercriminals the initiative, it is important for those involved in the fight against cybercrime to try to anticipate qualitative and quantitative changes in its underlying elements so that they can formulate their methods appropriately. The importance of being acquainted with the effects of cyber crime keeping in mind the recent activities that have taken place and offering solutions to protect an individual and/or an organization from them is laid down in this paper. Types of cyber security and cyber attacks are listed in this paper. It also throws light on the state of cyber crimes and cyber security in India. A gist of Indian cyber laws is presented in this paper as well.

Key words: Cyber Security Cyber Crime, Information Security, Cyber threats, attacks, Hacking, Phishing, Cyber Safety, cyber prevention and detection.

1. Introduction

Our life is becoming more digitalized with the rapid technological developments. Be it business, education, shopping or banking transactions, almost everything is on the cyber space today. The attention being given to cyber security is often focused on trying to define the problem and assess the true threat level. Cyber security plays an important role in the development of information technology as well as Internet services. Cybercrime is evolving at an astounding pace, following the same dynamics as the inevitable penetration of computer technology and communication into all walks of life. In information technology data protection or information security is one of the great challenges for the world. It is one of the serious issues in information industry. Internet is one of the important and very fast growing commodities for development of business as well as in different private and government organizations. It is being used as the largest communication and information exchange medium now. At the same time Internet is becoming an instrument of numerous types of cyber crimes. It is being used to steal and manipulate the information of users. Important data is being stolen and personal as well as organizational threats are being imposed upon the users which are using Internet. Sensitive information, secret credentials and even the bank account details are being stolen these days with the use of Internet. Cyber security is becoming a serious issue for the complete world with intruders attacking people or organizations with the motive of getting access to their restricted content.

Cyber attackers are enjoying a renaissance with the increasing availability of bandwidth, connected devices, and affordable attack tools that allow them to launch ever-more complex and potent attacks against a cyber security practitioner's (CSP's) residential subscribers and businesses. The threat to cyber security is growing at vast rate. Cyber criminals are becoming more sophisticated and are now targeting consumers as well as public and private organizations. Cyber crimes are rising due to the lack of cyber security. Many researchers have reported[1-3] the issues related to cyber security in past. This paper is an attempt to look at this issue for the whole world in general and for India in particular.

Joseph Migga Kizza defined[4] cyber security in terms of three elements;

1. Confidentiality
2. Integrity
3. Availability

Cyber security commonly refers to following three issues:

1. Precautionary activities and other measures, technical and/or non-technical, intended to protect computers, computer networks, related hardware and device software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the personal as well as national security;
2. The degree of protection resulting from the application of these activities and measures;
3. The allied field of specialized endeavor, including research and analysis, aimed at implementing those techniques and upgrading their quality.

Cyber security breaches have broad impact on almost all the stake holders of ICT. Some of these major impacts are as follows:

- Customers are subject to personal identity theft, fraud, and inferior, bogus or pirated goods.
- Businesses risk losing corporate secrets, intellectual property, benefits of new innovations, corporate reputation, and profits through espionage and breaches.
- For a nation's broader economy business and individual losses impact GDP, reduce economic growth and innovation, and result in a smaller tax base.
- For governments, espionage and cyber attacks threaten national security and diplomatic relations.
- Critical infrastructure that provides traffic signals, water, power, food supply, and healthcare are becoming more attractive targets for attacks.

1.1. Where does cyber security come from?

Cyber security is a complex issue that cuts across multiple domains and calls for multifarious initiatives and responses. It is generally believed that cyber security began in 1990s but in-fact viruses and worms have been part of the background noise of cyberspace since its earliest days. For instance in the movie War Games (1986) a young teenager hacks his way into the computer that handles command and control for the US nuclear arsenal. The famous Cuckoo's Egg incident in the mid-1980s made the people to understand that foreign spies had found innovative ways to procure highly classified information. Cyber security gained momentum in the 1990s with the advancements in science and technology. Access devices had multiplied and diversified to include a variety of portable and wireless accesses. Cyber security professionals typically use multiple endpoint tools to protect their customers from common cyber threats. Each tool generates alerts based on a particular kind of suspicious activity. Most organizations only have the resources to investigate 4% of alerts. It is upto the organizations to select the vulnerable alerts and put the rescue team on task. Undoubtedly it requires an attentive and alert cyber treats response team. Needless to say the organizations will have to compromise between threats and costs, and here the cyber criminals start getting an edge over the cyber security personnel.

2. Aspects or Types of Cyber Security :

There are several types of computer securities that are completely based on protecting from different types of viruses, worms and Trojans[5-6]. Some authors called them aspects of cyber security. The common types of computer security are as follows;

2.1 Network Security :

This is a common type of computer security which deals with securing the networks, that is from privately owned computer networks to the internet itself against different types of viruses and also many other forms of threats to keep the working of computer networking smooth. Having set the right kind of network security assures the stable working of computer network. As the data are available only for authorized users, it is possible for hackers to pretend to be one, by providing the correct user name and password thereby disrupting the computer network security.

2.2 Data Security :

Another important form of the computer security is the data security. It is defined as the act of protecting the important data present on the computers from different types of threats through various software/hardware solutions such as Antivirus and firewalls. This data can either reside in one or more computer storage devices or be exchanged between two or more computer systems. It affects mostly, confidentiality, integrity and availability of information.

2.3 System Security :

It mainly concerns about malicious programs that can disrupt and sometimes destroy the computer systems. These malicious programs can be viruses such as Love Bug, rabbits, Logic Bomb, Trojan horse and worms such as Morris Worm and, bugs. If attackers succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims. **Ransomware** is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. Ransomware malware can be spread through nasty email attachments, infected software apps, infected external storage devices and hacked websites. Once executed in the system, ransomware can either lock the computer screen, or, in the case of crypto-ransomware, encrypt predetermined files. Ransomware is considered "scareware" as it forces users to pay a fee (or ransom) by scaring or intimidating them.

3. Types of cyber attacks :

Researchers have studied and reported[7-10] various types and classes of cyber attacks. Major types are as follows:

Table 1: Types of cyber attacks

Passive Attacks	disclosure of the confidential information or the files to an attacker takes place without the consent of the concerned person or the authority
Active Attacks	hackers attempt to make changes to the data on the target machine
Denial of Service	users are deprived of access to the network or its resources
Close-In Attack	an individual or a group is trying to attain close proximity to networks so that, they can modify, collect the information or deny the access to the information
Phishing Attack	the bait is thrown out with the hope that while most will ignore the bait, some will be tempted into biting
Exploit Attack	the attacker takes the advantage of a particular vulnerability that system offers to the intruders when the intruder knows about the security problem within an operating system or in a piece of software
Password Attack	Password attacks are the classic ways to gain access to a computer system to find out the passwords and login Ids

4. Important Cyber law Provisions in India :

Many authors have reported about the cyber treats, attacks and various other issues in Indian context[11-18]. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of digital solutions has also given birth to a range of new age crimes that are addressed by the Information Technology Act, 2000.

The **Information Technology Act, 2000** (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the fundamental law in India dealing with cybercrime and electronic commerce. The original Act contained 94 sections, divided in 13 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India. A major amendment in this act was made in 2008. It introduced the Section 66A which penalized sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". At the same time it also introduced penalties for child porn, cyber terrorism and voyeurism. It was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha.

Major provisions of this law are as follows[19]:

Table 2: Major provisions of Information Technology Act, 2000 and Amendment, 2008

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to Rs. 2,00,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to Rs. 5,00,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to Rs. 1,00,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to Rs. 1,00,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to Rs. 1,00,000
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to Rs. 2,00,000
66F	Acts of cyber terrorism	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	Imprisonment up to five years, or/and with fine up to Rs. 10,00,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to Rs. 10,00,000
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to Rs.10,00,000 on first conviction. Imprisonment up to seven years, or/and with fine up to Rs. 10,00,000 on second conviction.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to three years, or/and with fine up to Rs. 2,00,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to three years, or/and with fine up to Rs. 1,00,000

In India, at least one cyber attack was reported every 10 minutes in the first six months of 2017 [20]. In the first quarter of 2017, as per the Indian Computer Emergency Response Team (CERT-In), a total of 27,482 cases of cybercrimes have been reported across the world. With the higher percentage of cybercrime coming forward this year, this number is expected to shoot up in future. India stands 11th in the ranking for cyber crime in the world, with a toll of 3% of total global cyber crime[21]. United States of America being technologically strong country is having various advanced techniques and tools to prevent the cyber crimes but at the same time USA itself is having a forecast for spread of around 7.41 million new malware specimens in 2017. It is easy to see that the cyber criminals are moving few steps ahead of the cyber security personnel. According to National Crime Record Bureau (NCRB) the total number of incidents of cyber crime in India was 50,300 in 2016. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 44,679, 49,455 and 50,362 cyber security incidents were observed during the year 2014, 2015 and 2016, respectively. A total of 5,693, 9,622 and 11,592 cyber crime cases were registered during 2013, 2014 and 2015, respectively. A remarkably growth can be seen in the number of cases registered in 2016 (50,300)[22].

The National Informatics Centre (NIC) was set up in 1975 with the prime goal of providing IT solutions to the government. It is the prime nodal agency In India to provide IT services to the governmental organizations. It has played a pivotal role in steering e-governance applications in the governmental departments at national, state and district levels, enabling the improvement in, and a wider transparency of, government services. Almost all Indian-government websites are developed and managed by NIC.As in most countries around the world, the cyber security scenario in India is one of relative chaos and a sense of insecurity arising out of the periodic reports of cyber espionage, cyber-terrorism, cyber warfare and cyber crime. A detailed report on Indian status in the area of cyber security has been presented by Institute for Defense Studies and Analyses (IDSA) through its Task Force Report India's Cyber Security Challenge[23]. This report has presented the Indian cyber scenario, loop holes, steps required to face Internet war (IW) and Cyber War (CW) in very systematic manner. It has also proposed a probable structure of office which may be required to play the key-role in case of IW and CW. Recently, the governments of India and the US have signed a Memorandum of Understanding (MoU), promising close cooperation and exchange of information around cyber security issues.

5. Prevention Methods for Cyber Crime :

Cybercrime prevention can be easy- when equipped with a little technical advice and common sense, many attacks can be avoided. Online criminals, in general are trying to make their move successful as quickly and easily as possible. They will be forced to search for easier targets if we make their job more difficult by the use of cyber security tools.

The best methodology for fighting against cybercrime is through education and enforcement of laws as well as highly developed security services. Technical expertise in online security is necessary, which can ensure that people of all the ages and fields are always safe. Cyber prevention is the act of restricting, suppressing, destructing, destroying, controlling, removing, or preventing the occurrence of cyber attacks, in either, computer systems both hardware and software systems, networks and data, or any other electronic devices capable of being a computer from such attacks.

Prevention is always better than cure. It is always better to take certain precautions while operating the net. It is strongly prescribed to take the following steps to prevent cyber crime:

i. Choose strong passwords and keep them safe. Use separate ID/password combinations for different accounts, and avoid writing them down. Don't use passwords that are easily accessible, i.e., that contain names, birthdays, phone numbers, etc.

ii. Disclosure of personal information publicly on websites must be avoided.

iii. Make sure to change your login details, at least once or twice a month. You can cut down your chances of being a target of cybercrime by doing so.

iv. Avoid sending photograph(s) online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

v. Avoid entering your credit card number and other bank account credentials to any site that is not secured, to prevent its misuse.

vi. Always use latest and updated Antivirus software to guard against virus attacks.

vii. Always keep back up of your data to prevent loss of data due to virus attacks.

viii. It is strongly advised to use a security program that gives control over the cookies and send information back to the site, as leaving the cookies unguarded might prove fatal.

ix. Use of network firewalls proves beneficial.

x. Ensure that your social networking profiles (e.g. Facebook, Instagram, Twitter, You Tube, MSN, etc.) are set to private. Check your security settings and be careful what information you post online.

xi. Generally we leave our mobile devices unattended. By activating the built-in security features we can avoid any access to personal details. Try to avoid storing passwords, pin numbers and even your own address on any mobile device.

xii. Use encryption for your most sensitive files such as health records, tax returns, and financial records. Make regular backups of all of your important data.

xiii. Don't click on a link or file of unknown origin. Check the source of the message; when in doubt, verify the source.

6. Management of Cyber Security Risks :

The risks associated with any cyber attack depend on three factors:

i. threats (who is attacking and to what extent),

ii. vulnerabilities (the weaknesses they are targeting upon), and

iii. impacts (what are the results of the attack).

The management of risk is considered fundamental to effective cyber security.

6.1 What are the Threats?

People who actually or potentially perform cyber attack are widely cited to fall into one or more of five categories:

- i. Criminal's intent on monetary gain from crimes such as theft or extortion;
- ii. Spies intent on stealing classified or proprietary information used by government or private entities;
- iii. nation-state warriors who develop capabilities and undertake cyber attacks in support of a country's strategic objectives;
- iv. "hacktivists" who perform cyber attacks for nonmonetary reasons; and
- v. terrorists who engage in cyber attacks as a form of non-state or state-sponsored warfare.

6.2 What Are the Vulnerabilities?

Cyber security is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by insiders with access to a system; supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix. Even for vulnerabilities where remedies are known, they may not be implemented in many cases because of budgetary or operational constraints.

6.3 What Are the Impacts?

A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. Cyber theft or cyber espionage can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. Denial-of-service attacks can slow or prevent legitimate users from accessing a system. Botnet malware can give an attacker command of a system for use in Cyber attacks on other systems. Attacks on industrial control systems can result in the destruction or disruption of the equipment they control, such as generators, pumps, and centrifuges. Online games which misguide the net or cell-phone users are also examples of cyber crimes. The effects of such games may be as harmful as committing suicide by the player or theft of secret credentials from the players' digital devices.

7. Conclusions

Despite being world-known as an information technology superpower, India lags far behind when it comes to official cyber security workforce which comprises a small number of experts deployed in various government agencies. Cyber security is becoming an indispensable dimension of information security. It can be concluded from this present study that with increasing rate of cyber crimes more detection techniques alongwith educating the users on being safe online needs to be established with complete guidance to know about the pros and cons of the web before entering it. One of the biggest security concerns today is the insider threat. Another major security concern is lack of consistency in enforcing "acceptable use" policy. Concrete measures must be found in order to track electronics evidence and preserve them so that systems are better protected from cyber intrusions. To defend against cyber crimes, intrusion detection techniques should be designed, implemented, and administrated. The way to protect it for now is for everyone to be smart and to follow preventive measures. Individuals, institutions, and governments should all follow these measures. It is the time that the countries of the world, including India, realise that a well-protected cyberspace would only be an asset to developing and developed nations. In view of the rapidly growing threats to national security in cyberspace there is urgent need for the governments to adopt well developed cyber security policies. Cyber security education, R&D and training should be an integral part of the national cyber security strategy. India is progressing in this area by implementing proper policies and by implementing well designed laws. The state as well as national governments are taking steps to prevent cyber crimes but the efforts have not been enough so far. There is still a need of developing a skilled and experienced task force. We need to expedite our efforts in this field as the threats of cyber crimes and cyber war are increasing exponentially day by day.

References

1. Tonge A. M., Kasture S. S., Chaudhari S. R., Cyber security: challenges for society-literature review, *IOSR Journal of Computer Engineering (IOSR-JCE),* e-ISSN: 2278-0661, p-ISSN: 2278-8727, *12(2),* 67-75 (2013).
2. Dunn M., The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP), *International Journal for Critical Infrastructure Protection*, *1 (2/3),* 58-68 (2005).
3. Stoll C., The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage, New York: Pocket Books (1990).
4. Kizza J. M., Guide to Complete Network Security, 4th Edition, Springer International Publishing, ISBN: 978-3-319-55605-5 (2017).
5. Agarwal K., Dubey S. K., Network Security: Attacks and Defence, *International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE), 1(3),* 8-16 (2014).

6. http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/ types-of attack.html.
7. Homer J., Zhang S., Ou X., Schmidt D., Du Y., Rajagopalan S. R., and Singhal A.. Aggregating vulnerability metrics in enterprise networks using attack graphs, *Journal of Computer Security, 21(4),* 561–597 (2013).
8. Zhuang R., DeLoach S. A. and Ou X., Towards a theory of moving target defense, *Proceedings of the First ACM Workshop on Moving Target Defense, ACM*, 31–40, (2014).
9. Cerrudo C., An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks; retrieved from https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf, accessed on 30.09.2017.
10. Stewart J. N., Advanced Technologies/Tactics Techniques, Procedures: Closing the Attack Window and Thresholds for Reporting and Containment, Best Practices in Computer Network Defense: Incident Detection and Response M. E. Hathaway (Ed.) IOS Press, 2014.
11. Prakhar Golchha, Deshmukh R. and Lunia P., A Review on Network Security Threats and Solutions, *International Journal of Scientific Engineering and Research (IJSER), 3(4)*, 2347:3878 (2015).
12. Kandpal V. and Singh R. K., Latest Face of Cybercrime and Its Prevention In India, *International Journal of Basic and Applied Sciences, 2(4),* 150-156 (2013).
13. Dashora K., Cyber Crime in the Society: Problems and Preventions, *Journal of Alternative Perspective in Social Sciences, 3(1),* 240-259 (2011).
14. Ayyuby S. and Agrawal P. K., “A Review on Dangers of Social Engineering and Some Possible Solutions,” Emerging Trends in Computer Science and Information Technology, Shabd Publications, Bhopal, India, ISBN: 978-93-85145-05-6.
15. Alpana, Malhotra S., Cyber Crime –Its types analysis and prevention Techniques, *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN-227128X, 6(2),* 145-150 (2016).
16. Maghu S., Sehra S. and Bhardawaj S., Inside of Cyber Crimes and Information Security: Threats and Solutions, *International Journal of Information & Computation Technology, ISSN 0974-2239, 4(8),* pp. 835-840 (2014).
17. Yassir A. and Nayak S., Cybercrime: A threat to Network Security, *IJCSNS International Journal of Computer Science and Network Security, 12(2),* 84-88 (2012).
18. Chitrey A., Singh D., Bag M. and Singh V., A Comprehensive Study Of Social Engineering Based Attacks In India To Develop a Conceptual Model, *International Journal of Information & Network Security (IJINS), ISSN: 2089-3299, 1(2),* 45-53 (2012).
19. http://www.itlaw.in/bareact/chapter-11-offences/ ; accessed on 30.09.2017
20. http://www.india.com/news/india/27482-cases-of-cybercrimes-reported-in-2017 -one-attack- in-india-every-10-minutes-2341055/; accessed on 30.09.2017.
21. https://www.slideshare.net/MOE515253/cyber-crime-ppt; accessed on 30.09.2017.
22. https://twitter.com/synclature/status/841567197495468032; accessed on 30.09.2017.
23. India’s Cyber Security Challenges by Institute for Defense Studies and Analyses, ISBN 81-86019-98-7; http://www.idsa.in/book/Indias Cyber Security Challenges; accessed on 30.09.2017.