AN INTRODUCTION TO CYBER CRIMES AND ROLE OF CYBER-SECURITY IN INFORMATION TECHNOLOGY

Jeevan Prasad Adhikari[1], Dr. Arvind Kumar Sharma[2]

Department of Computer Science and Engineering

[1,2]OPJS University, Churu (Rajasthan) - India

ABSTRACT

Cyber-attacks can significantly hurt an organization's IT environment, leading to serious operational disruptions, from simply damaging the first layers of IT security up to identity theft, data leakage and breaking down networks. Moreover, the dangers through which current cybercrimes practices affect organizations present a tendency of developing more rapidly that decision makers can assess them and find countermeasures. Because cyber threats are somewhat new thus a critical source of risks, within the context of the constantly changing IT environments (e.g. cloud services integration) organizations may not effectively implement and manage cyber threat risk assessment processes. This paper highlights the importance of designing effective security strategies and proactively addressing cybercrime issues as key elements within the organizational risk management approaches.

1. INTRODUCTION

Information Technology has developed hugely during the most recent two decades and turned into the fundamental wellspring of knowledge. The most recent information and the current technology make information accessible through the Internet. Information through the internet is helpful for amateur and furthermore to the master in all fields of knowledge. Information Communication Technologies (ICT) is the fundamental model of utilization for utilizing public Internet offices with a specific end goal to access information. In creating nations public and shared offices help to make urgently required access to information sharing and information access [1]. With regards to public access, Cyber Cafes assume a vital part as the most widely recognized Internet access display. Cyber Cafe is one of the real public access to ICT and have been contributing a considerable measure in the internet infiltration and to lessen the digital gap in India and all around the world. Despite the fact that Internet is a crucial wellspring of information, the Cyber-crimehas likewise expanded. The Owners of Internet cafes expand the opportunity for utilization of Internet access to the group yet they neglect to fix their PC security to shield the private information of their Visitors.

Cyber security management assumes a crucial part of Cyber Cafe Owners and Visitors. Consistently new dangers and cyber-assaults are made and occurring. Internet and PC utilized for it are getting

to be apparatuses for cyber-crime. Assaults by cyber offenders can be conceivably similarly as harming to the national foundation as assaults by fear-based oppressors. The momentous development of Cyber Café and Internet access has made the issue of Cyber-crime proliferation with the absence of solid confirmation bringing about examination challenges. These cyber dangers emerge because of vulnerabilities, the absence of Cyber security awareness and absence of Cyber security preventive measures taken while utilizing the internet cafe. This cyber security chance should be taken care of by recognizing dangers and powerlessness and the effects of these dangers. Existing laws for Cyber-crime are not up to the check since technology changes at a speedier rate, and each time new sort of Cyber-crime happens. The preventive measures taken by internet clients are not viable to keep away from Cyber-crime [2].

1.1 Globalization & Revolution in Information Communication Technology

Information Communication Technology (ICT) is a central point in the global mix emerging from the trade of things and thoughts. It frames a driving factor for globalization. Technology is developing at a colossal rate, new equipment, programming, and systems are enhancing step by step which helps in conveying at a speedier rate bringing about the development of the economy in all sectors. Worldwide coordination is a consequence of trade of thoughts, item, perspectives and assets among various countries for which communication

among individuals must be speedier [3]. Headway in ICT has given way to universal globalization paying little mind to the geographic area. ICT unrest is named as to process information in digital shape and impart it. ICT insurgency has enhanced the lives of numerous individuals in the general public. Society as entire is enhancing as far as benchmarks and enhanced the way of life with monetary development. Communication by making utilization of ICT is done through different courses, for example, messages, chat rooms, and sites, informing frameworks, for example, WhatsApp, Hike courier and so forth which has united individuals of same enthusiasm to accomplish their objectives and enhance their business. Organizations are thriving because of ICT since basic leadership is ending up speedier as the examination of information is done in less time traverse. Additionally, there is a reasonable rivalry between organizations staying away from imposing a business model of few organizations.

2. CYBER SPACE USAGE: WORLD AND INDIAN SCENARIO

Internet shapes prime component of cyberspace. It gives a situation to communication and trade of information and resources. Utilizing these condition individuals with unlawful reason can make false personality to conceal genuine character and cheat other individuals on the system. Cyber security awareness, ensuring the system foundation alongside reasonable measures to maintain a strategic distance from Cyber-crime is a

critical perspective that should be considered. As indicated by Department of Electronics and Information Technology, the internet is an effective apparatus that ought to be utilized for advancement of society and development of the economy [4]. The Internet is a key component of national foundation.Most of the internet users use internet without understanding the dangers associated with it. As per the technological changes the internet users need to update themselves frequently. Along with individual responsibility the government needs to take efforts for cyber security management and protecting the cyber space. In today's scenario the major factors for Cyber-crime and threats are lack of awareness, lacunas on technological aspects, poor management of cyber security, and lack of cyber security knowledge and careless attitude.

3. ICT INITIATIVES IN SMART CITIES

Smart Cities are new ideas that are developing everywhere throughout the world. IBM began with the idea of a smart city in their venture Smarter Planet Initiative in 2008, and gradually all country began thinking on a similar line. The greater part of the created countries began looking into for smart cities and contributed intensely to it. ICT has a vital impact on usage of smart cities. Smart cities make utilization of various technologies, for example, Wi-Fi, sensor technology, anyplace whenever communication and savvy frameworks to deal with the administrations required and to take care of the issues. It

additionally persistently chips away at future extension and difficulties for new and energizing smart city highlights. This requires on spot gathering of data, examining the data, distinguishing the dangers and vulnerabilities and risk related to it alongside appropriate risk management to be finished [5]. A portion of the featuring highlights of the smart cities incorporates steering the activity consequently without sticking, staying away from mischances, recognition of Cyber-crimes at a speedier rate, recognizing a place to stop the vehicle, demonstrating areas to clients, for example, hotspot, lodgings, air terminals and so on.

3.1 Social and Economic Impact of Cyber Cafe to ICT

Public access point like Cyber Cafe has an assortment of effects on ICT. Digital incorporation is the major impact and the other is social and financial effect. It is certain that individuals lacking access to ICTs will influence the economy of the nation. Cyber Cafe causes individuals to defeat restrictions, for example, absence of innovative abilities or neediness which influences the utilization of ICT and thus influencing the economy. From the viewpoint of users, utilizing computers and the internet at public access settings provides advantage in various angles in their lives which incorporate Education, Employment and Income, look into, Government work, and Communications Culture change by blog and sites, Travel and Entertainment. In this way it is certain that public access point, for example,

Cyber Cafe influences the countries and even individual lives as far as self-improvement, monetary growth and social prosperity [6].

Pune is an instructive center with parcel of youthful understudies examining in various fields. Pune was called "The Oxford of the East" by Jawaharlal Nehru India's first Prime Minister, because of the notable scholastic and research foundations in the city. There is developing requirement for internet association. This offered ascend to increment in Cyber Cafe for internet services. Additionally because of IT center point individuals are more mindful about security and make utilization of Cyber Cafe for different purposes, for example, explore, commercial reason, e-administration services and so forth. Today there are 259 registered Cyber Cafes in Pune city alongside numerous unregistered Cyber Cafe. The greater part of Cyber Cafe offers internet service to Visitors as far as broadband service and Broadband Wi-Fi.

3.2 Cybercrime and its escalation

Cyber-crime is a term in which criminal exercises are finished utilizing the medium of computers or computer systems. In this way internet, cyber space and the overall web can be utilized to perpetrate crime. The development of internet and the upheaval of crime begin together. The cyber criminals perpetrate demonstrations of crime and illegal follow up on the World Wide Web. Internet crime takes various structures, for example, Hacking, Phishing, Cyber

Vandalism, Spamming, Spoofing, DoS, Backdoor, and Trojan and so on hurting numerous individuals by badgering them, taking or altering their data, making hurt the information framework, ransacking cash by picking up their bank qualifications and numerous more [7].

3.3 Growth of cybercrime

United States stand first followed by Canada and on third position United Kingdom. Australia ranks fifth in Cyber-crime complaints registration. Cyber Criminals make use of different types of techniques to make scams to cheat Internet users. These frauds are of various types such as identity theft, lottery scam, Nigerian fraud or hacking and malicious software or malware scams. Some recurring and common crime schemes include Ransomware/Scareware Scams, Child Pornography Scare ware, Fake or Rogue Anti-Virus Software, Real-Estate Rental Scams, Work-at-Home (Employment) Scams, Identity Theft, Credit Card Fraud, Lotteries, Phishing and Spoofing.

3.4 Cybercrime in India

The Nation Crime Records Bureau (NCRB), Ministry of Home Affairs has indicated Cyber-crime Statistics for the year 2013, which obviously mirror that there is fast increment in Cyber-crime by 50 percent on year to year premise from 2012 to 2013. India stands fourth on the planet for Cyber-crime. In the year 2013 an aggregate of 5693 cases were registered under various Cyber-crime offenses and a sum of 3301 individuals were

captured.Cyber-crime in Maharashtra is becoming quick. According to a current Criminal Investigation Department (CID) Maharashtra 2013 report on crimes in the express, the expectation behind crimes can be vindicate, cash, hassling individual for the sake of entertainment or envy, want to offensiveness somebody or might be eve prodding. The report said that Cyber-crimes suspects as a rule were business contenders, remote nationals or grouping, despondent workers, programmers, understudies or expert students, neighbors, relatives or companions of casualties. Most extreme Cyber-crime happens because of lack of awareness about Cyber-crime and cyber security. Pune city Cyber-crime has ascended by 39.3 percent inside the city recording 319 cases till December 4 2014.

3.5 Present Cybercrime through Public Cyber Cafe

Cyber Cafe are public internet access point and it is discovered that public access point is the most loved places by cybercriminals since they can without much of a stretch hack the Visitors data because of lack of awareness of Cyber-crime in Visitors and in addition their character is hard to uncover as they are making use public internet point . Numerous Cyber Cafes are currently giving Wi-Fi services to their clients. Because of lack of awareness of Cyber security numerous Cyber Cafe Visitors commit errors, for example, making utilization of decoded devices or conventions, not logging out after work is

finished, straightforward secret word, same watchword for various locales, Information left on the hard drive, not clearing program history, putting away of data on public hard circle, not checking for illicit or vindictive software before utilizing public machine which brings about misfortune to the Visitors [8].

4. CYBER SECURITY

Information Technology has developed immensely in India in a most recent couple of years and is in charge of growth of the individual in each angle. It helps people in each stroll of life. Internet users have come to up to 100 million and broadband endorser has come to up to 12.69 million. India has developed in all a wide margin as far as internet associations with space name registration and increment in internet service suppliers. Today India has 134 major Internet service suppliers, million "in" areas and 10 million or more registered space names. Because of increment in internet use and cyberspace activities, there is additionally increment in Cyber-crimes or mechanical crimes in the nation. Alongside this lack of teaching from users, insufficient computer, and system framework protection, lack of Cyber-crime cyber security management and the mysterious utilization of ICT – enabling users to shroud their personality and furthermore conceal their tracks of crime. Information Technology Act 2000 is a legitimate system made and actualized to anticipate Cyber-crime and alterations have likewise occurred for it yet at the same time enhancements are required. Today Indian

cyberspace has an increment in spam and phishing activities, spread of botnets; infection, worms, and malignant code are additionally on rising. It additionally had security approaches in which different nations could collaborate to forestall Cyber-crime. Later the alteration act additionally appeared to defeat some security issues not considered in before Act alongside some new options of security aversion and lawful treatment of Cyber-crime. The government has IT Act, National Cyber Security Policy is a strategy structure given by Department of Electronics and Information Technology (DeitY), Ministry of Communication and Information Technology, Government of India [9].

4.1 Information Technology to Cyber Security

We take the simplicity of electronic instalments, internet requesting, and portable managing an account for allowed – that is until the point that you get hacked, or there is a security break. It can be overwhelming to realize that your MasterCard information is sitting in the hands of a mysterious hacker, and for organizations that get hacked, the stakes are likewise high. It can rapidly turn into a PR bad dream and, in particular, an organization can rapidly lose trust with its clients. However, the pressing requirement for cyber-security is making an abnormal state tech field that prepared IT aces can discover their way into on the off chance that they pick up the correct involvement. Organizations are hoping to contract individuals, instead of utilizing

software, to guarantee that their data and client information stays as private as would be prudent. Cisco directed a report on security and found that there is a lack of cyber-security masters for organizations to employ. The report likewise expresses that with a specific end goal to battle security dangers, organizations require individuals, not software or computers, to help ensure their organizations and clients.Be that as it may, as more individuals enter the information technology field, it is ending up more focused. You will need to guarantee you have a college degree in computer science or related field. However, Ira Winkler of Computer World prescribes that understudies don't have some expertise in Cyber security.

5. INFORMATION TECHNOLOGY CYBER SECURITY POLICY

This Cyber Security Policy is a formal arrangement of standards by which those individuals who are offered access to organization technology and information resources must withstand. The Cyber Security Policy fills a few needs. The fundamental objective is to advise organization users: workers, contractors and other approved users of their compulsory prerequisites for securing the technology and information resources of the organization. The Cyber Security Policy depicts the technology and information resources that we should ensure and recognizes a significant number of the dangers to those advantages. The Cyber Security Policy likewise depicts the client's duties and

benefits. What is viewed as adequate utilize? What are the principles concerning Internet access? The strategy answers these inquiries, portrays client constraints and advises users there will be punishments for infringement of the arrangement. This archive likewise contains strategies for reacting to episodes that undermine the security of the organization computer frameworks and system. It is the commitment of all users of the organization frameworks to ensure the technology and information resources of the organization. This information must be shielded from unapproved access, burglary, and pulverization.

6.   The   Role   of   Cyber-Security   in Information Technology

Is cyber-security real and what is its part of   Information   Technology?   What contrasts and connections exist between Information   Assurance   and   Security   and cyber-security? These are questions that have as of late been the point of some exploration   and   investigation   inside Brigham Young University's IT Program. The IT 2008 Model Curriculum perceives Information Assurance and Security as a key component of IT training with space both in the center and in the propelled educational modules. Inside the mainstays of IT instruction, it is set properly over the highest point of the five topical columns and   portrayed   as   a   coupling   string. Without a doubt, this is the approach wanted   by   numerous   scholastics   to guarantee   that   an   awareness   of   the requirement for security is imparted in

understudies in every single major course. Notwithstanding being an independent central   subject,   the   IT   2008   Body   of Knowledge   incorporates   security   as   a subtopic   of   Networking,   Social   and Professional Issues and Web Systems and Technologies.   This   unavoidable   cross-course guideline is a piece of the center instruction   offered   inside   Information Technology   with   further   developed subjects   and   strategies   prescribed   as cutting-edge level material. In particular, the model educational modules suggest that further developed IAS material be canvassed   in   the   fourth   year   as   an integrative affair to tie the components instructed inside every column. Numerous administration   bodies   have   been   long-lasting supporters of cyber-security and have   as   of   late   dedicated   noteworthy endeavours and resources to reinforcing their nations' cyber-pose. As a pioneer in this area, the US as of late reported their goal to sort cyber-assaults as acts of war [10];   in   the   meantime,   the   UK   declared another $1 billion (USD) activity to create progressed   mobilized   cyber-security capacities.

7. CONCLUSION

Cyber security has turned into a matter of global intrigue and significance. Effectively more than 50 nations have authoritatively distributed some strategy record plotting their   official   position   on   cyberspace, cybercrime,   and   additionally   Cyber security.The extraordinary points of view of   Computer   Science,   Computer Engineering,   Electronic   Engineering, Information Systems, Mathematics and

numerous different fields which share an enthusiasm for cyber-security, can add to making our digital society a more secure place.Information Technology exhibits an exceptionally suited and perfect condition for cyber-security instruction that separates it from different disciplines. To be sure was one to plan a separate train particularly for cyber-security; we trust it would nearly take after an Information Technology program with a cyber-security accentuation.

REFERENCES

[1]   GadgeReena K., Dr.MeshramB.B.,"Detect and Prevent Threats in Websites"- IJCST-International Journal of computer science and Techno- vo l. 3, Issue 1, Jan. - March 2012 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

[2]   HaseloffAnikar M. - "Cybercafes and their Potential as Community Development Tools in India "- The journal of community informatics - Vol-1 No-3 2005 - http://ci-journal.net/index.php/ciej/article/view/226/181 - 12/5/2014

[3]   Sife. Alfred S -" Internet use behavior of cybercafé users in Morogoro Municipality, Tanzania"- Annals of Library and Information Studies Vol. 60, March 2013, pp. 41-50

[4]   Lunt, B. M., Ekstrom, J. J., Gorka, S., et al., Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. Association for Computing Machinery (ACM); IEEE Computer Society, November 2008.

[5]   BBC, US Pentagon to treat cyber-attacks as 'acts of war'. British Broadcasting Corporation, June 1, 2011. http://www.bbc.co.uk/news/world-us-canada-13614125 (Last Accessed: June 1, 2011).

[6]   BBC, UK beefs up cyber warfare plans. British Broadcasting Corporation, May 31, 2011. http://www.bbc.co.uk/news/technology-13599916 (Last Accessed: June 1, 2011).

[7]   Spacewar.com, White House proposes new cybersecurity bill. Space War, May 12, 2011. http://www.spacewar.com/reports/White_House_proposes_new_cybersecurity_bill_999.html (Last Accessed: June 1, 2011).

[8]   Schneier, B., Worst-Case Thinking. Schneier on Security, May 13, 2010.

[9]   Falliere, N., Murchu, L. O. and Chien, E., W32.Stuxnet Dossier. Symantec, February 2011.

[10] Weishäupl, E., Yasasin, E., and Schryen, G. 2015. "IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review," in ECIS 2015 Completed Research Papers