Development and impact of cyber crime

CYBERCRIME: A FIGHT AGAINST CYBER PERPETRATORS

ABSTRACT

With the introduction of the internet, awareness of people has increased manifoldly due to increase in the access to knowledge, by just a click away. Despite all the benefits of internet, certain issues do persist and one of them being cybercrime. In this paper, I would like to discuss about the evolution of cybercrime, the drastic changes which are incurring with the advent of technology as the days pass by leading to rise in risks, and finding what the encouragement factor for the cyber perpetrators is. Next, discussion being on the victimization of younger generation at individual level that how the victims are targeted by criminals leading to loss of personal identity details and financial loss whereas if we talk about the targets towards the organizations, it leads to inside crime, malicious registrations of domains and e-waste generation. Lastly, measures which should be adopted, if not for complete eradication but at least leading to minimization of cybercrime at all the levels possible.

INTRODUCTION

Regardless to the commercialization of the Internet and other new information and communication technologies just two or three decades prior, various types of cybercrime have turned into a daily event. The focus of its violations extends from government and multinational enterprises to people, hence leading to an extensive variety of research enthusiasm in regards to the potential ramifications (Näsi, Oksanen, Keipi &Räsänen2015, pp. 203-210)

“ Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes)”. “ Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitive or malicious purposes”. “ Criminals who perform these illegal activities are often referred to as hackers” (Geetha & Phamila 2016, p. 58).

As indicated by the Global Cyber Executive Briefing, it was normal that “ virtually all organizations will be attacked” and in this way top corporate administrators “ need to better understand their biggest threats and which assets — typically those at the heart of their business’s mission — are at the greatest risk” (*Cybercrime: No Bajan business is safe 2014).*

Due to the rise of cybercrime extensively and having a 100 percent guaranteed defence against cyber-attacks is next to impossible. One needs to combat the threats created by the digitization of internet in the society for a safer and secure environment among people (Pupillo 2013, pp. 151-152, 159).

In this review I would like to discuss about how to cybercrime got evolved, threats that are targeting the vulnerabilities such as to younger generation at individual level and the business or government organisations at large, whereas how various measures can be undertaken to combat the cybercrime.

EVOLUTION OF CYBERCRIME (WHAT ENCOURAGES THE CYBER PERPETRATORS?)

As per Alstin (2016, p. 2) the concept of computer virus was very alienated term for many in the early 2000 when the internet was being adopted. Whereas, when at schools teachers used to discuss regarding computer viruses, it was very difficult to comprehend what they were trying to reference and various thoughts used to emerge in the mind that why would someone squander resources on such a thing. As the years passed by the term cybercrime began to be more actively used in headlines i. e. " hospitals and health systems held hostage by computer programs launched by elite cybercriminals", moreover Alstin (2016, p. 2) on the other hand talks about the Symantec 2016 Internet Security Threat Report which denotes how much drastic change has occurred in cybercrime and " organizations that have made cybercrime their business, intelligently designing software to more effectively cripple their targets and undermine defences".

The worldwide technology scene was altogether different in the late spring of 2010: Nokia was the pioneer in smartphone industry, NASA had joined hands with Rackspace to learn more about cloud computing, and Intel was prepared to obtain McAfee to end up distinctly an overwhelming hitter in the cybersecurity world. Steak forward to today " Intel says, it underestimated the rapid evolution of cybercrime over the past five years" and highlights how the attacks have risen with the advent of new technology these days *(ICT Monitor Worldwide* 2015).

Martin (2015, pp. 207-220) has examined that " The incentives in cybercrime are classic in that they encourage attack and discourage defence" as a result cybercrime generates higher returns at a reduced risk which ultimately incurs less cost for the hackers. Moreover the exploitation techniques such

as “ social engineering” in which the hacker “ cybercriminal tricks a user into granting access” whereas the “ vulnerability exploitation” technique where the “ hacker gains advantage by a programming or implementation failure to gain access”. The fact that risk and cost involved in a cybercriminal activity is very low, it becomes irresistible for hackers to not victimize someone even if the rate of return per victim is favourably low (Martin 2015, pp. 207-220).

VICTIMIZATION OF YOUNGER GENERATION (INDIVIDUAL LEVEL)

Cybercrime at an individual level often arises due to victimization by a known assailant, and if we compare the figures of cybercrime victimization, they were higher in the younger generation than the older generation. According to Oksanen and Keipi (2013, pp. 298-309) “ 2. 5% of respondents aged 15-74 years reported being victims of cybercrime in 2008 and among the ages of 15-24, the figure was 5. 3%.”

Ever since 2007, the Australian Institute of Criminology has recorded data on online personal fraud by doing some online surveys of the scam invites received by victims during the last 12 months and the outcome being, 95% of them reported being a victim of online scam invitations and 8% of the total lost around $8, 000 per head which turns to be a total of $846, 170. The most frequent types of scam being fraudulent lotteries and emails, as reported by 72% people. The ones who were financially affected by this scam, 61. 5% of those were females, 36. 8% were men and the remaining 1. 7% were the ones who didn’t disclose their gender.

An interview of 750 victims of a cybercrime was done in United Kingdom to understand how it affected them, to which 68% had emerged a feeling of

anger, 45% were traumatised by monetary loss, 44% were stressed out and 37% faced psychological imbalance. For instance, as per BBC News (2008) an online Nigerian lottery fraud happened in which a Chinese student after reaching England for study had incurred a loss of £6, 000 or more had committed suicide under pressure due to the scam in Nigeria.

Furthermore re-victimization is also creating a huge issue for the victims because once their details (financial and personal) are received by the perpetrators, they include all that in a list called “ sucker list” through which another fraudster can defraud the person again by a scheme called “ recovery fraud” in which the victim is approached online to recover the money lost at the first place (Cross, Cassandra, Smith, Russell G, Richards & Kelly2014).

A report was released by Symantec supported by a market research company StrategyOne, gathering votes of 77000 individuals of various nations to evaluate their notions on cybercrime, of which 65% respondents were victims of cybercrime and only 44% of them lodged a complaint to the police. There were various concerns of under reporting like it’s a shear: wastage of time and effort and again a survey done by Symantec proved that 80% of the voters didn’t expect the cybercriminal getting caught. Moreover no one wants to be a victim because there is no chance of getting help from the police due to lack of resources most of the times, whereas there is neither any “ motivational reward” for reporting such crime, rather the victims are called fools to fall for such traps, which ultimately results in “ negative, rather than positive reinforcement” (Goucher 2010, pp. 16-18).

TARGETING THE BUSINESS/GOVERNMENT ORGANISATIONS

Cybercrime does not solely targets an individual, huge businesses are also a targeted and in such a case the victim has a greater reason to keep shut because a firm has a certain reputation in front of their customers and the top management won't be willing to disrupt that by portraying unethical acts which might hamper the customer's data. So, in such a case the employee who has been affected by a cybercrime and is already under huge pressure and stress, might be willing to commit crime against the employer as well and extract the required money for his/her own condition. For instance, banks instruct the managers how to tackle with situations like when their family is threatened to compromise with them for an ' inside crime', but whatever the case maybe the persons priority will always be towards the welfare of their family and the bank is affected more or less (Goucher 2010, pp. 16-18).

Now if we talk about online fraud in media, Deloitte has analysed certain ventures of online media are most vulnerable to cyber threats and undermines the status of various organisations which were facing rising complex attacks which includes various government agencies as well (*Cybercrime: No Bajan business is safe 2014).*

A report has been prepared by Jacksonville (2016), focusing on a case in which 81 companies in Financial Times Stock Exchange 100 (FTSE 100) who had " potentially malicious domain registrations against them, enabling cyber criminals to create dummy websites that can be used to trick users into supplying private data." There were 527 dummy domain names

registered which ultimately targeted the brand and the credential information of an organisation. What actually happened was the employees of FTSE 100 compromised the official email and password combination for other purposes like for gaming websites etc., in total 100 out of 5275 emails and passwords were compromised for the hackers to gain access to the potentially important and sensitive information of those companies.

As published by Martin (2015, pp. 207-220) another issue which has emerged these days is of cyber threats caused by e-wastes which act as a medium of leaking the highly confidential information of various government organisations. For example, In Ghana certain hard drives were purchased online from eBay comprising information of US military defence system, to which an analysis was made by some researchers, and they found that 160 computer hard disks had been purchased from various nations like United States, the United Kingdom, Australia & Germany, and they could extract readable data from only 60 drives, which contained 48% information regarding the organisation, 53% regarding certain individuals and 5% of that information was examined as unlawful. The reason being for all this was due to ignorance towards “ in-house” recycling.

MEASURES TO COMBAT CYBERCRIME

Cyber security does not solely reply on the IT department of an organisation. All the other departments should also be proactive towards it. Keeping this in mind Cybercrime Response Strategy (CRS) should be adopted in a workplace to keep a track of the threats faced by employees and organisation (Kenya 2014).

Security awareness training should be provided to individuals in an organisation for their own as well as the organisation’s benefit, by encouraging them to keep themselves and their family protected by being aware regarding the various cyber threats. Moreover, intimating the organisation about any security issues which arise so that required steps can be taken within time (Goucher 2010).

Cybercrime Response Strategy (CRS) is one of the important areas where investment should be prime focus in an organisation due to its great dependence on management and technology for communication, to maintain the firm’s ICT infrastructure for cyber-crime detection and prevention process (Kenya 2014)

Furthermore for cyber related crimes various legal actions need to be formulated for taking legal action against the cyber criminals. For example, Cybercrime bill in Thailand has been passed despite various criticism for the betterment of the country in terms of improved online monitoring (*Thailand: ICT to revise Computer Crimes Act to handle cybercrime* 2014).

The other case being of Nigeria, as said by Martin (2015, pp. 207-220) various measures have been undertaken by them to establish the Economic and Financial Crimes Commission (EFCC) in 2004 which adopted a cyber security bill in 2011 following various objectives such as: “ provide an effective legal framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria” and “ enhance cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs in Nigeria”.

CONCLUSION

Cybercrime is and will continue to be one of the most important topics in the area of information security within the next years. Due to the ongoing digitalization of society, companies are continuously shifting more and more activities to the Internet, leading to increased number of attacks (Konradt, Schilling & Werners 2015).

When an individual is targeted by the cyber perpetrators, it leads to loss of personal identity details and in some cases even financial losses are incurred which needs to be reported but due to lack of action by the police they tend to avoid doing so.

Whereas if we talk about organisations, it involves the issues faced by both an individual as well as the organisation. The issues faced are such as inside crime, malicious domain registrations & e-wastes generated, and all of them require proper awareness training, limited use of work related credentials outside the office and proper in house recycling is required.

Moreover the measures to combat such crimes should be taken such as implementation of Cybercrime Response Strategy (CRS) by organisations, and on the other hand government should also take some legal steps for the prevention of cybercrime so that the criminals don’t feel free to commit such crime. At the end we can just hope for a better and more secure digital environment.

REFERENCES

Anomali updates on cyber security vulnerabilities of FTSE 100 companies. (2016). *Entertainment Close – Up* , Retrieved fromhttps://search-proquest-com. ezproxy. lib. swin. edu. au/docview/1794323097? accountid= 14205

Cross, Cassandra, Smith, Russell G, Richards & Kelly(2014 *). Challenges of responding to online fraud victimisation in Australia* . Woden: Australian Institute of Criminology. Retrieved fromhttps://search-proquest-com. ezproxy. lib. swin. edu. au/docview/1537383140? accountid= 14205

‘ Cybercrime: No Bajan business is safe’ *ICT Monitor Worldwide* , 11 July 2014, ezproxy. lib. swin. edu. au/login? url= http://go. galegroup. com/ps/i. do? p= ITOF&sw= w&u= swinburne1&v= 2. 1&id= GALE %7CA377105696&it= r&asid= f78b32378a5da9d9c93fb30b3ea7d635. Accessed 24 Mar. 2017

Doyon-Martin, J 2015, ‘ Cybercrime in West Africa as a Result of Transboundary E-Waste,’ *Journal of Applied Security Research* , vol. 10, no. 2, pp. 207-220.

Geetha, S & Phamila, AV 2016, *Combating security breaches and criminal activity in the digital sphere* , Information Science Reference, Hershey, PA.

Goucher, W 2010, ‘ Being a cybercrime victim,’ *Computer Fraud & Security* , vol. 2010, no. 10, pp. 16-18.

‘ How to curb cybercrime threats in organisations.’ *Business Daily* [Nairobi, Kenya], 17 Mar. 2014, ezproxy. lib. swin. edu. au/login? url= http://go. galegroup. com/ps/i. do? p= ITOF&sw= w&u= swinburne1&v= 2. 1&id=

GALE%7CA377144848&it= r&asid= a26c756f51a5c9f84fce0bd9a8b2266c. Accessed 24 Mar. 2017.

Intel: We underestimated the rise in cybercrime *.' ICT Monitor Worldwide* , 2 Sept. 2015, ezproxy. lib. swin. edu. au/login? url= http://go. galegroup. com/ps/i. do? p= ITOF&sw= w&u= swinburne1&v= 2. 1&id= GALE %7CA427476725&it= r&asid= c868a3d3e3fcd17c5a8279438c651e40. Accessed 19 Mar. 2017

Konradt, C, Schilling, A & Werners, B 2016, ' Phishing: An economic analysis of cybercrime perpetrators,' *Computers & Security* , vol. 58, pp. 39-46.

Michael Van Alstin, Chad 2016. ' The evolution of cybercrime: Why aren't we evolving with it? Why aren't we evolving with it?' *Health Management Technology* , June 2016, p. 2, ezproxy. lib. swin. edu. au/login? url= http://go. galegroup. com/ps/i. do? p= AONE&sw= w&u= swinburne1&v= 2. 1&id= GALE%7CA456706201&it= r&asid= 6a1e481e8da12284640b1880a60ef744. Accessed 19 Mar. 2017

Näsi, M, Oksanen, A, Keipi, T & Räsänen, P 2015, ' Cybercrime victimization among young people: a multi-nation study,' *Journal of Scandinavian Studies in Criminology and Crime Prevention* , vol. 16, no. 2, pp. 203-210

Thailand: ICT to revise Computer Crimes Act to handle cybercrime', *Asia News Monitor ,* 26 Sep, viewed 19 March 2017, http://search. proquest. com. ezproxy. lib. swin. edu. au/docview/1564712809? accountid= 14205&rfr_id= info%3Axri%2Fsid%3Aprimo