TYPES, PREVALENCE, AND PREVENTION OF CYBERCRIME

Haya Fetais & Mohammed Shabana

Saint Leo University

COM- 510

November 23, 2014

Introduction

Globalization and technological developments have infiltrated into every fiber of modern day living. In the modern era, it is possible for business transactions to be carried out by individuals who are on different continents on the planet. It is also possible for a single individual to be the CEO of a company which has branches all across the world. Entertainment, social life, and education are all areas which have benefited greatly from technological advancement. However, there are also the negative effects associated with these developments.

Cybercrime or cyber insecurity is the greatest of these vices. There are different forms of cybercrime that are explored in this paper. Cyber bullying is one of the crimes where individuals often harass others through the internet. There is also the aspect of hacking in which unauthorized individuals get to access information that is confidential. This leads to stealing of business ideas, business strategies, and even personification. Worse still, cyber terrorism has also become quite popular. Since the 9/11 attacks on the US, the anti-terrorism units became quite vigilant. In order to continue raining terror on the people, the terrorist groups have gone technological where they hack government and institutional sites, causing internet outage or even changing the information therein.

Given the nature and spread of the cybercrimes and the fact that the internet is here to stay, it is important to evaluate the various efforts that are put in place to prevent cybercrime. Cyber surveillance is one of the methods. The collaborative approach is one of the most effective strategies that can be applied where different governmental organizations, private institutions, and other players come together to curb this threat. These strategies will be further explored in the paper.

Types and Prevalence of Cybercrime

There are many types of cyber crimes, but most of them can be basically divided into three major categories, which are (Main Types of Cybercrime):

1. *Cyber crimes against persons:*

   This type of cybercrime is against persons and individuals with the use of a computer such as E-mail. There are many different kinds of this type of cybercrime such as drug trafficking and offensive content & Harassment. For example, in March 1999 it was the first time where the Melissa virus appeared and after that it spread dramatically throughout the computer systems in the United States of America and Europe.

2. *Cyber crimes against property:*

   This type of cybercrime is where the target are all forms of property and it also includes computer vandalism and transmission of harmful programs such as, Electronic funds transfer fraud and dissemination of offensive materials. For example, "A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyber spy" (Harpreet, 2013).

3. *Cyber crimes against government:*

   This type focus on cyber crimes against government and cyber terrorism where individual or a group attack any governmental database to help them steal something or plan for a

terrorism attack. Examples of this type are (electronic vandalism and extortion) and (cyber warfare and terrorism).

Moreover, after dividing cybercrimes into three categories here are the top five most prevalence cybercrimes that cybercriminals try to do the most according to American institute of CPAs, IBM, Computer Security Institute (CSI), and more other sources (Singleton, 2013):

1. Tax-refund Fraud
2. Corporate Account Takeover
3. Identity Theft
4. Theft of Sensitive Data
5. Theft of Intellectual Property

Tax-refund Fraud:

In this kind of cybercrimes, cybercriminals use a valid name and social security number for a person who will not fill for tax return. They will get this information by using social engineering, email phishing, or maybe purchasing the data from the black market where sellers in the black market have some kind of access to personal information of many persons. They might also be working in a high traffic business such as hospitals or car dealerships where they can get such information.

After that cybercriminals will make up the rest of the information such as wage and withholding information and then file the fraudulent tax return electronically because with electronically filled tax returns the W-2s are not included and that will give them more time to

file more fraudulent tax returns and by the time IRS discovers this the crime will be already completed.

However, all taxpayers could be the next victims of tax-refund fraud because it is not that hard for cybercriminals to find ones personal information form the Internet or other sources and use it against them.

Corporate Account Takeover:

Cybercriminals use software to hijack remotely one of the computers that are inside a bank or a financial company and steal funds or transfer money to other account. This can be done in three steps: the first one is illicitly acquire login credentials and that can be compromised by using a malicious program. This program will be distributed as an email attachment or a file transfer and it will look like a safe file. The user will accidently allow the malicious program to be downloaded and executed. The second step is to gain unauthorized access to the victim's computer to avoid any security features. Most of the hackers use some tools to hijack the victim's computer system in order to use the system as a trusted source to avoid any security check. The third step is to transfer the victim's bank funds to a secure account controlled by cybercriminals.

For this kind of crimes Small and medium businesses are the targets because they care less about information security, so they are easy target for cybercriminals.

Identity Theft:

It typically happens when cybercriminals steal one's personal data and this data has financial benefits. Some of the malicious purposes that cybercriminals are looking for when steal personal data are: opening a line of credit, obtaining employment, receiving medical care, purchasing goods or services, and/or renting or buying a house or apartment.

Gathering the data for identity theft occurs the same as in tax-refund fraud by social engineering or from the black market where most of cybercriminals buy their data from it.

Theft of Sensitive Data:

It is similar to identity theft, but in this type sensitive data such as unencrypted data like credit card information and customers information stored by a business. The difference between this type and identity theft is the costs to victims will be higher and involve public-image damage and financial costs related to loss of business.

The crime in this type of cybercrimes occurs when cybercriminals get access to sensitive data and then they steal it and store it in a different device. After that they use the data they got to transfer money or other data they need to a secure account.

Theft of Intellectual Property:

There is many other information or even things can be stolen by cybercriminals such as books, movies, and music since they are copyrighted materials. In addition, cybercriminals

access these materials and then they distributed it for free without complying with copyright laws.

Prevention against Cyber Crime

According to Dashora (2011), cyber crimes have been at the heart of criminal activities for such a long time. This is mostly because the individuals, companies, or government agencies that are targeted by the cyber criminals do not have effective strategies to protect themselves from the attackers. It is, therefore, important to make sure that there are effective strategies that can be put in place to keep the vulnerable targets from such forms of violation. Dashora (2011) further indicates that with cyber crime, the best mode of prevention is through pro-active rather than reactive measures. This implies that the targeted individuals have to identify the possible routes through which they can be invaded and then make the necessary arrangements to make sure that they do not fall victims. With regard to this, there are two levels of protection that can be adopted as discussed below.

Protection of Individuals:

This is the level of protection, which seeks to secure individuals from falling victims of cyber attacks. The forms of cyber crimes that can be prevented at this level include identity thefts, cyber bullying, hacking into personal profiles and accessing private information, and other similar offences. These are the offences that are directed towards individuals.

Dashora (2011) indicates that there are some strategies that can be put in place so as to prevent such crimes. First of all, it is important for the users to be educated and aware of the

possible routes through which they can be affected. As such, they would try by all means possible to avoid being in such situations. These include strategies such as avoiding using computers in a public set-up where other individuals can easily see what the individual is doing. Secondly, it is important to have strong passwords to individual accounts such as e-mail and other social sites. This can make it hard for the hackers to get access into an individual's private domain.

Individuals should also secure their computers. This implies that whenever an individual uses a personal computer (PC) to access the internet, the firewall should be activated. This can help in ensuring that the computer is blocked from connections that can be a route of entry for viruses and hackers. This is the first line of defense when using a computer on the internet and is very effective in protecting individuals. Other applications that the individuals can use to protect themselves include use of antivirus or malware software as well as blocking of spyware which can infiltrate and disrupt the functioning of an individual's PC.

Above all, Human (2014) indicates that the only sure way that an individual can be protected from cyber crime is by making sure that there is responsible use of the internet. This implies that the users understand that there is always the threat of cyber attacks. As such, they are ever vigilant in making sure that they do not give a loophole through which the attackers can infiltrate. Further, it is important to make sure that all profiles created on the net are in private mode as this can help in making sure that there are no chances of access by unauthorized individuals.

Protection of Corporate Organizations and Governmental Departments:

While protection of individuals is a little bit easier, it is more difficult to protect the governmental and corporate organization from cyber crime. This is explained by Morrison (2014) who indicates that such are the main targets of terrorists and other corporate criminals. Further, this route of attack can be used in cyber warfare by different countries in conflict where one infiltrates the governmental sites of the other and changes information, or even causes a total network outage in the target countries. This form of crime is high profile and, therefore, needs high profile prevention tactics. There are three main approaches that can be employed to prevent this type of cyber crime.

Offensive Defense:

Morrison (2014) defines this mode of prevention as the mode of prevention by attack. This seeks to prevent companies and governmental departments from hackers as well as computer malware. It is based on understanding the mechanism by which the hackers or malware providers work. In order to hack or introduce malware into a system, the intruders need to work in a given domain and then introduce the virus into the system through mail or any other available route of entry. Offensive attack involves invading the network of the attackers and compromising it such that they can no longer carry out their activities. The US department of Homeland Security has used this mode of prevention on several occasions. The most notable is when the government-made Trojan Horse virus was introduced into the system. This worked well in ensuring that those planning attacks on the governmental sites would be stopped in their tracks by the surprise invasion of their networks by the government. Although this form of defense can be very effective, it is quite expensive since it needs the use of expertise and

computer literacy. It is, therefore, an expensive but effective approach in dealing with cyber crime.

Collaborations:

One of the biggest challenges that face the corporate industry and the governmental agencies when it comes to cyber protection is that there is no definite understanding of where the danger could come from. The cyber attackers keep the possible targets guessing and wondering where the next attack could come from or even where it would be targeted. As such, a lot of the potential victims keep on guessing and coming up with different protection strategies. Human (2014) indicates that working in collaboration is the best approach that can be adopted by the victims. Rather than one company or departmental agency coming up with a protective measure and keeping it to itself, there should be sharing of information such that discovery by one of them serves to protect everyone else. This, therefore, would ensure that any discovery in the field does not lie dormant in only one location. Further, such a strategy ensures progress in ensuring cyber security because the there is no duplication of efforts. It also helps to make the targets more prepared for any eventuality because they have a lot of options to explore in case of an attack. While this approach might be effective, it is highly dependent on the level of trust between the collaborating partners. It is also a bit tricky because there could be possibilities of some partners taking advantage of the others. To prevent such an eventuality, it is important to have Memorandum of Understanding (MOUs) amongst the partners so as to make sure that everyone so effectively covered and that none takes advantage of the others.

Cyber Surveillance:

Just like with the other forms of protection against terrorism, intelligence is very important in preventing cyber attacks. This, therefore, implies that it is vital to collect intelligence that can help in foretelling possible plans of the intruders. Morrison (2014) indicates that this can be a very effective strategy. However, this strategy has to be carried out by government authorized agencies, such as the Department of Homeland Security, CIA, FBI, and other protection agencies. This approach is employed when there is a possibility of cyber terrorism taking place.

Morrison (2014) indicates that after the 9/11 attacks, the US put in place this measure through the US PATRIOT Act which allowed the intelligence units to collect electronic data from internet users. Through this authorization, the surveillance activities were carried out in collaboration with service providers where wire communications of individual were tapped into. Of course, the strategy brought about much controversy as many people felt that their privacy was being invaded and that their rights were being violated. However, the rights of the individual are not superior to the security of the nation and therefore the intelligence collection went on. This serves to show how sensitive this strategy of cyber crime prevention is, and justifies why it has to be carried out by state authorized bodies.

The strategy involves collecting internet traffic in collaboration with the internet service providers (ISPs). It helps in knowing the source and destination of given information and helps in interjecting should there be a need to.

Since the intelligence is very vital in making cyber security decisions and increasing situational awareness, there are qualities that the intelligence should contain. First, it needs to be accurate. This is because decisions can be made from such information. Therefore, there are no chances for erroneous information as it can lead to misinformed decisions. Secondly, at has to be timely. This means that the intelligence has to come at such as time that it helps the concerned parties to act proactively. Otherwise, if the information is delayed, it might be of no use as the damage could be done already. Lastly, the information should be complete as this is the only way through which it can help in ensuring making of the right preventive decisions.

Conclusion

Though the Internet is a discovery whose benefits cannot be denied, it has also brought about various concerns, including concerns about cyber security. A lot of cyber crimes have been reported, ranging from cyber bullying to corporate crime and cyber terrorism. This brings about the need for prevention of the cyber crimes. The review above has revealed that cyber crime can be prevented through strategies such as individual awareness, offensive prevention, collaborations, and cyber surveillance. Whatever the method of prevention, the key factor underlying cyber crime prevention is by acting proactively; preventing the damage before it is done.

References

Dashora, K. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in Social Science*, Vol. 3(1), pp. 240-259.

Harpreet Singh Dalla, G. (2013). Cyber Crime - A Threat to Persons, Property, Government and Societies. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5). Retrieved November 20, 2014, from http://www.ijarcsse.com

Human, D. (2014). Veteran Private Investigator Steps Up Cyber Sleuthing. *Indianapolis Business Journal*, Vol. 35(20), pp. 3-25.

Main Types of Cybercrime. (n.d.). Retrieved November 20, 2014, from https://sites.google.com/site/callingoffcybercrime/goto/home

Morrison, D. (2014). FBI Report Undercovers Roots of Cyber Attacks. *Credit Union Times*, Vol. 25(6), pp. 8.

Singleton, T. (2013). The top 5 Cybercrimes. Retrieved November 20, 2014, from http://www.aicpa.org/Pages/default.aspx