ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (409-414), Month: April - June 2015, Available at: www.researchpublish.com

Cyber Crime and How It Can Be Counteracted

Marwan Ali Albahar

Abstract: **Cyber crime has been on the increase in the recent past, calling for an investigation into the area to point out the challenges that are surrounding it. This paper, acknowledging that with the advancement in technology, computer application in many social, economic as well as political arenas seeks to propose and discuss some actions that if taken can help in the fight against cyber crime. The platforms under which the methods can work to the best of performance are also delved in the course of the paper. The paper notes that mobile devices and the application development for the mobile devices is a loophole that cyber criminals effectively are making use to commit crime on the internet. It that dedicates a good part of it to discuss how mobile devices and application development can be used to counter cyber crimes Further, this paper addresses the use of some peculiar principles, the use of programs that are designed to counter cyber crimes, policy design and where necessary strengthening, use of network regulation as well as educating the larger public and enforcement of the designed laws to ensure that the crimes associated with computers are brought into control. The necessary details required for effective implementation of each of these methods and or mechanisms are thoroughly explained in the paper to leave no room for unclear concepts or points. In doing this, the paper integrates the roles of the company and individuals, in the spheres ranging from ethical concerns to professional inputs that are called for in the war against cyber crime.**

Keywords: **Cyber crime, application, investigation, application.**

1. INTRODUCTION

The world has seen a remarkable transformation in commerce with the advent of Internet based companies. Goods and services are routinely purchased and delivered electronically leading to significant changes in industries like journalism, travel, and banking. Online payments (eBilling and ePayments) cut across all industries and are being used by a significant portion of U.S. households. For example, eBay reports that literally millions of people make their entire living solely on the eBay platform.

Clearly, a large portion of the population relies on the Internet, either directly or indirectly, for an ever-increasing set of services. Technology devices such as computers, laptops, mobile phones, IPods among other devices are all being used on daily basis to enable people access the information that is stored on the internet. The world has become a global village and seemingly nothing can slow this trend, with the possible exception of some catastrophic failure of the internet. It is unlikely that the Internet as a whole will experience such a catastrophic technical failure, and in fact it is the believe of this study that these borders on the impossible. Cyber crimes, and other online attacks have evolved as the key challenge that online business and other activities are experiencing. If these are left to become widespread, crowd psychology could take hold and similarly to the recent global financial crisis, lead to a loss of faith in "the system". It turns out that cyber crime is something that needs to be dealt with in a serious manner not only by private or government organizations, but also in conjunction with all the nations of the world taking part in the process because this is not an individual nation's problem but a problem of the entire globe.

This paper explains that cybercrime is slowly getting worse and those technical measures alone, while necessary and helpful, cannot significantly move the trend line in a positive direction. Kunz and Wilson (2004) observe in a report presented to the University of Maryland that "The past several decades have brought a vast increase in the availability of electronic resources. With this increased availability has come a new form of criminal activity that takes advantage of electronic resources, namely computer crime and computer fraud. Currently, these new forms of crime are burgeoning and pose a new and lasting challenge to law enforcement agencies at all levels in how to prevent, investigate, and prosecute

these crimes (Kunz and Wilson 2013, p. 3)." There is much data to support this position, and it is no use neither helpful to simply regurgitate that here. Baseline, action is called for in order to counteract this negative trend, and we present arguments in favor of a multi-faceted regulatory approach to dealing with the problem, as the only viable way to proceed in the long-term.

The central fact is that cyber crimes have been on the increase of late, and especially with the technological advancements that are being witnessed every now and then. The impact of the cyber crimes are serious and in some cases may result in suicide or high levels of depression. It translates to the fact that it is essential for cyber crimes be delved into in details, in order to minimize the impact associated with them. It is for this reason that this topic on cyber crime was chosen for this research study. The study, as mentioned earlier, intents to bring some light to the entire spectrum of those involved and how the vice can be possibly controlled if not stopped. The methods as well as the laws of accessing the website will be explained in details in the research study. Taking into consideration that mobile devices that can access the internet have become readily available, this paper closely offers some mechanisms in which such devices can be useful in the war against cyber crime.

2. PROBLEM STATEMENT

2.1 The Problem:

Cybercrime, just like all other forms of crime, is a multi-faceted and ever-changing problem. As such, this research study does not intent to exhaust the entire spectrum of the possibilities that there are with regard to dealing with the seemingly fast growing vice of cyber crime. Rather, this study will propose a set of principles and actions which the researcher hopes that and believes they will have significant impact if adhered to and implemented. To give the study some stable background, several specific issues in the space of cyber crime are introduced and briefly discussed. To start with, this study acknowledges that there are various acts that fall in the "cyber" kind of crimes. Many solutions are bound to fail, as Allan (2013) observes, if the solution are bound to be varied. A proper understanding of each of these terms as relates to cyber crime is thus crucial to make things easier when it comes to solving the problem. A distinction of the terms is thus important. Before addressing these terms, a brief explanation of the impact that cyber crime has both on the local and global computing environment.

2.2 Security Impact on the Local and Global Computing Environments:

The impact of cyber crime to the local and global computing environments is so clear that it just needs to be highlighted here. The world has become a global village and thus many activities, including business, education, relationships formation and many other aspects relating to humans are all being done over the internet. With cyber crime, many of these aspects of human have been threatened and some cases the victims lose a lot of money, especially in the e-commerce world. Cyber bullying has caused many individuals, especially young ones to commit suicide when they cannot bear with the effect of cyber bullying. At the organizational and individual level, loss of private data has been witnessed in many instances, causing the victims great losses when they cannot recover the data.

2.3 Terms Relating To 'Cyber' Problem:

Cybercrime

Cybercrime is criminal generally an activity of using computers and the Internet to steal, whether directly or indirectly, from consumers or businesses. The global extent of the cybercrime problem is not clearly defined, but possibly involves a number of billions of money.

Cyber-espionage, by individual or groups

Cyber-espionage can be defined to be the process of hacking into personal computer systems in order to steal information. The hackers do this because they believe that the information has some useful information regarding the owners.

Cyber-warfare

The difference between cyber-terrorism and cyber-warfare has three dimensions, namely: scale, intention and actor. Intention targets to ruin resources whether economical communication or even those employed for essential online services.

Cyber-terrorism

Cyber-terrorism are attacks against directed towards one or more parts of the Internet with intentions of preventing rightful from accessing Internet-based services. The effect is fear to the user that the internet service is compromised and its integrity cannot be credited.

Cyber-espionage, by state actors

This is similar to the above-explained term, with some basic differences being motivation behind the intrusion ant the possibility that the range of reactions can be extreme in case the intrusion is publicized.

3. DESIGN AND USE OF RESISTANT MOBILE APPLICATIONS

3.1 Consider Available Applications:

Mobile devices are a breakthrough point for most cyber criminals. Heather Kelly in the article (Kelly, 2013) *Cyber-Criminals is targeting phones and bank info* observes that "Smartphones and tablets are increasingly hot targets for cyber-criminals, and the volume of mobile threats is growing much faster than it did for PCs. The amount of malware detected by McAfee on the devices in 2012 was 44 times what it was the previous year (Kelly 1)." Several reasons support this fact. In the first place, the cyber criminals are much aware that there is plenty of information these devices and as such, by use of viruses they can gain access to the information and extract the kind of details they want. As Kelly explains, the major cause is the applications that are upcoming and commonly used in these mobile devices. She writes in the article that "But McAfee's worldwide chief technology officer, Mike Fey, warns against looking at the number of threats targeting Android and assuming that other platforms are safer. Criminals are targeting the operating system partially because it is so open, and also because they tend to focus on the platform they think will be around the longest (Kelly 2)."

This point out to the fact that mobile devices are an area that needs to be thoroughly examined in the efforts to combat cyber criminals. A number of avenues exist as to how mobile devices and their development can be used in this fight, but the most significant per this study is the proper design of the applications that are used in these devices. "In order to address all these threats, Fey said, the industry needs to rethink security from the ground up, designing more secure products from the start instead of just constantly chasing threats (Kelly 4)"

3.2 Coding for Stability:

Having identified that mobile devices through the applications that are used in them go a long way to enhance cyber crimes, it narrows down to the fact that strong codes or applications need to be a matter of concern to every mobile application developer. When applications are being developed they should be integrated with stability features so that it can discourage the hackers and attackers who commit crimes through the computer.

4. THE USE OF PRINCIPLES

4.1 Identification and Discussion of Principles that Work:

In developing a series of recommendations for change, this study lays out a realistic set of principles that should underpin them. Some of them, when keenly considered, are practical and others conceptual. They are as follows:

1. Include the least regulation changes called for to attain appropriate levels of safety

It is the believe of this study that this principle is self-evident: do no more than need in order to make the Internet safer.

2. Make safety a priority

Many laws that apply to activities on the Internet, such as the U.S. Electronic Communications Privacy Act (ECPA) came before the internet reached the extent it is in today. As a result laws like ECPA often have basic scope problems that cause unintended consequences. Making safety a priority principle will help see the necessary changes in these laws implemented in order to match the nature of the problem at the present.

3. Make changes that minimize negative externalities in the overall

If your device is compromised through an attack by virus or malware, the negative effects may be noted by other person rather than you. As such, you do not have direct incentive to sufficiently protect your device. When you connect a device into the Internet, it is important to ensure that it is properly updated an of some sound safety levels.

4. Acknowledge the global nature of the internet and match what needs to be matched

No question about it, the internet is a global platform where everyone goes for information and other purposes. This implies that making laws against cyber crime in a give country stronger than in others will cause the crime to be directed into other nations with less jurisdictions with regard to it. A global stand needs to be taken by governments in order to deal with the vice as a globe.

5. Let governments in overall leave technical management of networks

The impact of this will be to ensure that only those properly aware of what really happens are involved and dedicated to management of technical points of the internet access mechanisms. Governments in most cases tend to generalize solutions and this could be really fatal in the fight against cyber crime.

6. Improve security but do not compromise privacy

This will help maintain the standards that have so far been attained but still cause improvements than calling for a full restricting of the entire internet platforms and computing systems used in many places globally.

5. POLICY DESIGN AND IMPLEMENTATIONS

5.1 Policy Design:

Policies should be designed with consideration being made to all that involves the safety of the users of the internet, mostly y use of mobile devices. For the policies to be effective, a number of factors such as their ethical soundness, professional soundness and legal soundness should all be integrated in their design. If they meet these requirements and are implemented by the right channels having been followed, the war against cyber crime will be progress well.

5.2 Policy Implementation:

Design of the policies alone is not enough, they will have to be implemented and where necessary enforced by some legal means. This is the only way that the designed policies will be useful and help to curb the vice of cyber crime. Various stakeholders should be involved in the implementation of the designed policies. These could include government, company leaders, parents to children who are many of the times victims of cyber abuse as well as the individuals who work for organizations as well as children. This will be a move targeting to make every individual aware of what needs be done in order to succeed in countering cyber crime.

6. NETWORK REGULATION

6.1 Make Customers aware of Malware:

The reason so many people fall prey for the cyber criminals is because there are no sufficient knowledge to enable them identify which applications are harmful to their personal computers. It should be the core interest of every organization and company, private and government alike, to ensure that the customers who use their networks are aware of the malware that can harm them. Customers should be made aware of how to identify the genuine sites and thus avoid sites that put their private information at risk.

6.2 Screen Criminal Traffic:

At the present moment many transit providers do have programs within their networks that can monitor the traffic passing through the network. This they achieve by inspection of the internet protocol addresses and as such this is a mechanism that can be useful for organizations to filter off criminal traffic from the network. If the criminal encounter this a number of times, they might get discouraged and this will help to minimize the number of cyber criminal attacks that happen over the internet.

6.3 Constrain Traffic within networks that perform IP Spoofing:

Noting that in today's computing world computers can be employed in the so called distributed denial of service within the networks, it becomes crucial that network designers restrict traffic to networks that have some mechanisms that can do a verification of the internet protocol address. Further, network service providers should and must ensure that the relevant IETF recommendations are strictly followed for network ingress and egress filtering.

7. EDUCATION AND LAW ENFORCEMENT

7.1 Education:

First there is a need to improve the consumer awareness on the threats that may occur in the internet world. Research studies show that most of the internet users have the least know how on how to protect themselves online. The government as well as the private sector has been involved in this topic, but there needs to be improvement on the topic. It is evident that the problem is much bigger relative to the scope of the work happening today. Most of the people are under fear of entirely using the internet even when they have a pressing need because they just do not know how to protect themselves. Thus, improving the steps that have taken to in educating the public on internet protection mechanisms. The educational efforts that are occurring today are good; they are simply not at the scale needed to help hundreds of millions of Internet users. This area needs significantly increased investment both from private industry and government. It is hard to know how much additional funding is needed, but it is quite possible that the right answer is "an order of magnitude" higher. New Internet users are coming online at a new generation. Introducing internet security in schools can also help.

7.2 Law Enforcement:

Fundamentally, it is the believe of this study that the relative investment in law enforcement for cybercrime is too low as at the present, as relative to the investment in law enforcement for regular crime. While it is undoubtedly true that there are financial thresholds imposed in prosecutorial decisions for regular crime, these are typically quite low. Thus, in most cases, if an individual steals, a minor property in the real world might end up being prosecuted unlike a guy who teals billions of money over the internet.

8. COMPANY AND INDIVIDUAL RESPONSIBILITY

8.1 Professional Responsibility:

Training of the company members on the awareness of cyber crime is one of the ways that the company can demonstrate professional responsibility with regard to combating cyber crime. For the devices that the company uses to connect to the internet, professional inspection should be done to ensure that they meet the requirements and that they are not faulty. Those found faulty should be forced out of the internet as these can be break points for cyber criminals into organizations networks to do harm. The members of the organization by observing these regulations and ensuring they do not connect to networks by use of substandard devices, especially mobile phones, will in overall show some professional responsibility in the war against cyber crime

8.2 Ethical Responsibility:

In lines of ethical responsibility, the company as well as the individuals can do a number of things to ensure that cyber crime is brought under control. The rules the company sets aside should be ethically sound so that by having its members follow them, they also demonstrate some ethical responsibility geared toward combating cyber crime.

8.3 Legal Responsibility:

Organizations should play a legal role in combating cyber crime by adhering to the rules and restrictions that have been provided by the government. Any company should ensure that it sets aside the stipulations of precisely what are the consequences of not adhering to ant-cyber crime regulations by any member of the organization. The leaders and administrators of the company should be at the fore front with regard to adhering to these regulations, as this will see the lower ranking members of the company follow suit and in overall help reduce the impact of cyber crime. The individuals can demonstrate legal responsibility by observing the set rules and by reporting any law breakers as pertains to cyber crime.

9. CONCLUSION

The foregoing and the issues that have been addressed in this paper point to the fact that cyber crime is something that needs to be dealt with in a serious manner. The problem of cyber crime has great impact on businesses, relationships and other areas that are associated with local as well as global computing environments. As at the present, several challenges are in place and hinder the rate at which this vice is being dealt with, causing many individuals and organizations alike to fall victims to this malpractice. This translates to the fact that the efforts to curb cyber crime is not an individual's work,

whether at personal level or organizational levels, but a task that calls for input of all the stake holders at the national and international arenas if the fight is to be won and cyber crime brought to control.

A lot has been done to combat cyber crime as of at the present. However, more needs to be done and this study has offered some of those actions that can be taken in order to minimize the impact of cyber crime. Mobile devices and the applications that are used in them are a very potential avenue for which criminals are passing to commit crimes over the internet and the computing world in overall. It is as such that this study proposes that in the attempt to solve this problem starting at the mobile devices and a strengthening of those applications used in them can go a long way in preventing cyber crime. Monitoring of networks to ensure that no criminal traffic flows, application of certain principles, educating the public as well as law enforcement are other possibilities that can add to what is already done with regard to dealing with cyber crime.

It is important that individuals and organizations as well do know their role and responsibilities that can help in combating cyber crime. These should be at the professional, ethical and legal responsibilities points of view. It is the view of this study if all this is put into consideration and that if all stakeholders take and play their roles effectively, the war against cyber crime can be won and make computing environments at the local and global levels alike a safe and secure activity.

REFERENCES

[1] Allan, K. (2013). Beating Cyber Crime: Security Management Program from the Borad's Perspective. EY , 4-17.

[2] Center, T. N. (2000). The Growing Global Threat of Economic and Cyber Crime. Lexis-Nexis Solutions Group , 24-36.

[3] International, K. (2011). Cyber Crime- A Growing Challenge for Governments. Issues Monitor , 1-15.

[4] Kelly, H. (2013, February 21st). Cyber-criminals are targeting phones and bank info. Retrieved July 17th, 2014, from CNN Tech: Cyber-criminals are targeting phones and bank info

[5] Lin Jiang, Z. H. (2013, December 11). Australia's Policies and Practices in Combating Cybercrime. Retrieved July 15th, 2014, from Australian Studies in China: https://www.library.uq.edu.au/ojs/index.php/asc/article/view/2017

[6] n.d. (2012). The Impact of Cyber Crime on Business. Penomon Institute Research , 15-22.

[7] n.d. (2011). Top Ten Ways to combat Crime on the Internet. Computer Crime , 1-6.

[8] Office, H. (2010). Cyber Crime Stategy. Cm , 20-32.

[9] Rowley, K. (2014, April 12th). Cybercrime and How it Affects You. Retrieved July 19th, 2014, from Vermont: Information Security: http://itsecurity.vermont.gov/featured/cybercrime

[10] Snow, G. M. (2010, July 28). The FBI's Efforts to Combat Cyber Crime on Social Networking Sites. Retrieved July 18th, 2014, from FBI: http://www.fbi.gov/news/testimony/the-fbi2019s-efforts-to-combat-cyber-crime-on-social-networking-sites

[11] Thostenson, L. (2012). Stopping Cyber Crime. CM Journal , 1-6.

[12] Wilson, M. K. (2004). Computer Fraud and Computer crime. New York: University of Maryland.