http://www.inosr.net/inosr-arts-and-humanities/
Geoffrey
INOSR ARTS AND HUMANITIES 4(1): 6-10, 2018.

International Network Organization for Scientific Research ISSN: 2705-1676

Cybercrime and its Effect on the Society, Understanding the Impacts.

Geoffrey Columbus

Department of Arts and Humanities Study, Faculty of Arts, University of Hong Kong.

ABSTRACT

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission. Cyber criminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Various categories like cyber-trespass, cyber-deceptions, cyber-pornography and cyber-violence is been used to classify types of cybercrime. Cyber crime affects society in a number of different ways, both online and offline, therefore various preventive method can help protection individuals against hackers in line with government policies against cybercrime .Keywords: Cybercrime, hackers, exploitation and government policies.

INTRODUCTION

As consumers increasingly allow technology into their personal lives, this technology stores and builds on troves of private data. Criminals take advantage of technology in many different ways [1]. The Internet, in particular, is a great tool for scammers and other miscreants, since it allows them to ply their trade while hiding behind a shield of digital anonymity [1]. Cyber crime is any criminal act related to computers and networks which is called hacking, phishing, spamming or is used as a tool to commit an offence (child pornography and hate crimes) conducted through the Internet. It is a bigger risk now than ever before due to the sheer number of connected people and devices. Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission. Cyber criminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage [1]. Criminals who are engaged in these illegal activities are often referred to as hackers. Common types of cyber crime include online bank information theft, identity theft, online predatory crimes and unauthorised computer access. More serious crimes like cyber-terrorism are also of significant concern. Cyber crimes cover a wide range of activities, but these can generally be broken into two categories such as crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks, and crimes that use computer networks to advance other criminal activities. These types of crimes include cyber-stalking, phishing and fraud or identity theft. Criminals committing cyber crime use a number of methods, depending on their skill-set and their goal [2]. Cyber crime, as distinguished from computer crime, is an umbrella term for various crimes committed using the World Wide Web, such as, theft of one's personal identity (identity theft) or financial resources, spread of malicious software code such as computer viruses; use of others' computers to send spam email messages (botnets), Denial of Service (DoS) attacks on computer networks or websites by the hacker, activism, or attacking computer servers of those organisations felt by the hacker to be unsavoury or ethically dubious, cyber stalking by which sexual predators use Internet chat rooms, social networking sites, and other online venues to find and harass their victims, cyber bullying, where individuals are harassed by others, causing severe mental anguish, cyber pornography, the use of the Internet to spread child and adult

pornography; Internet gambling and software piracy and cyber terrorism, the use of the Internet to stage intentional, wide-spread attacks that disrupt computer networks, using the Internet to spread violent messages, recruit terrorists, and plan attacks. Cyber crime affects society in a number of different ways, both online and in the offline world [2].

TYPES OF CYBERCRIME

Cyber crime can be divided into four sub-categories namely:

1. cyber-trespass (hacktivism, viruses, Denial of Service attacks)
2. cyber-deceptions (identity theft, fraud, piracy)
3. cyber-pornography
4. cyber-violence (cyber bullying, cyber stalking).

The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations. The broad range of cyber crime can be better understood by dividing it into two overall categories [3].

Type 1 cyber crime:

(a) Usually a single event from the perspective of the victim.
(b) Phishing is where the victim receives a supposedly legitimate email (quite often claiming to be a bank or credit card company) with a link that leads to a hostile website. Once the link is clicked, the PC can then be infected with a virus.
(c) Hackers often carry out by taking advantage of flaws in a web browser to place a Trojan horse virus onto the unprotected victims' computer.
(d) Any cyber crime that relates to theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

Type 2 cyber crime:

(a) Type 2 tends to be much more serious and covers things such as cyber-stalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.
(b) It is generally an on-going series of events, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship.
Eventually, the criminal exploits the relationship to commit a crime. Or, members of a terrorist cell or criminal organisation may use hidden messages to communicate in a public forum to plan activities or discuss money laundering locations, for example.
(c) More often than not, it is facilitated by programmes that do not fit under the classification crime ware. For example, conversations may take place using IM (instant messaging) clients or files may be transferred using File Transfer Protocol (FTP).

IMPACTS OF CYBER CRIME

The impacts of a single, successful cyber attack can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cyber crime on society and government is estimated to be billions of dollars a year. Criminals take advantage of technology in many different ways [4]. The Internet, in particular, is a great tool for scammers and other miscreants, since it allows them to ply their trade while hiding behind a shield of digital anonymity. Cyber crime affects society in a number of different ways, both online and offline.

Identity Theft

Becoming the victim of cyber crime can have long-lasting effects on life. One common technique scammers employ is phishing, sending false emails purporting to come from a bank or other financial institution requesting personal information [4]. If one hands over this information, it can allow the criminal to access one's bank and credit accounts, as well as open new accounts and destroy credit rating.

SECURITY COSTS

Cyber criminals also focus their attacks on businesses, both large and small. Hackers may attempt to take over company servers to steal information or

use the machines for their own purposes, requiring companies to hire staff and update software to keep intruders out. According to EWeek, a survey of large companies found an average expenditure of $8.9 million per year on cyber security, with 100 per cent of firms surveyed reporting at least one malware incident in the preceding 12 months and 71 per cent reporting the hijacking of company computers by outsiders [5].

MONETARY LOSSES

The overall monetary losses from cyber crime can be immense. According to a 2012 report by Symantec, more than 1.5 million people fall victim to some sort of cyber crime every day, ranging from simple password theft to extensive monetary swindles. With an average loss of $197 per victim, this adds up to more than $110 billion dollars lost to cyber crime worldwide every year [5]. As consumers get wise to traditional avenues of attack, cyber criminals have developed new techniques involving mobile devices and social networks to keep their illicit gains flowing.

PIRACY

The cyber crime of piracy has had major effects on entertainment, music and software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars per year [6]. In response, copyright holders have lobbied for stricter laws against intellectual property theft, resulting in laws like the Digital Millennium Copyright Act. These laws allow copyright holders to target file sharers and sue them for large sums of money to counteract the financial damage of their activities online.

SOCIAL IMPACTS

Cyber criminals take full advantage of anonymity, secrecy, and interconnectedness provided by the Internet, therefore, attacking the very foundations of our modern information society. Cyber crime can involve botnets, computer viruses, cyber bullying, cyber stalking, cyber terrorism, cyber pornography, denial of service attacks, hacktivism, identity theft, malware, and spam [7]. Law enforcement officials have struggled to keep pace with cyber criminals, who cost the global economy billion annually. Police are attempting to use the same tools cyber criminals use to perpetrate crimes in an effort to prevent those crimes and bring the guilty parties to justice.

Computer-related crimes date back to the origins of computing though the greater connectivity between computers through the Internet has brought the concept of cyber crime into public consciousness of our information society. "Billions of dollars in losses have already been discovered. Billions more have gone undetected. Trillions will be stolen, most without detection, by the emerging master criminal of the twenty-first century-the cyberspace offender" [7].

EMOTIONAL IMPACT OF CYBER CRIME

A new study by Norton reveals the staggering prevalence of cyber crime. About 65 per cent of Internet users globally, and 73 per cent of US Web surfers have fallen victim to cyber crimes, including computer viruses, online credit card fraud and identity theft. As the most victimised nations, America ranks third, after China (83 per cent) and Brazil and India (76 per cent). The first study to examine the emotional impact of cyber crime shows that victims' strongest reactions are feeling angry (58 per cent), annoyed (51 per cent) and cheated (40 per cent), and in many cases, they blame themselves for being attacked. [8] Only 3 per cent don't think it will happen to them, and nearly 80 per cent do not expect cyber criminals to be brought to justice resulting in an ironic reluctance to take action and a sense of helplessness.

Despite emotional burden, the universal threat and incidents of cyber crime, people still aren't changing their behaviour - with only half (51 per cent) of adults saying they would change their behaviour if they became a victim. Even fewer than half (44 per cent) reported the crime to the police. Nearly 80 per cent of cyber crimes are estimated to originate in some form of organised activity [8]. The diffusion of the model of fraud-as-service

and the diversification of the offerings of the underground market are also attracting new actors with modest skills. Cyber crime is becoming a business opportunity open to everybody driven by profit and personal gain.

APPLICATION OF THE CYBER CRIMES THEORY

Based on the child exploitation as one among cyber crimes, the Routine Activity Theory (RAT) is applied to this study [9]. The theory focused on environmental "opportunities for crime". Essentially, when a potential criminal opportunity arises the act will occur at a juncture in time and space between a motivated offender and a suitable target for victimization. This crime will ultimately take place in a location that lacks a capable guardian to protect the 'suitable target,' which is considered to be either a vulnerable person or one's unguarded property. Thus, the absence of any one of these three situational factors should theoretically make the commission of a crime impossible. As a result, routine activity theory is considered to be a macro-level theory applicable to numerous types of crime as it seeks to explain the criminal victimization process and not a criminal's specific motivations [9]. The theory predicts that crime occurs when a motivated offender comes into contact with a suitable target in the absence of a capable guardian that could potentially prevent the offender from committing crime. Ngo and Paternoster (2011) said that, the theory posits that variations in crime rates could be explained by the supply of suitable targets and capable guardians, and from our understanding the theory is somewhat agnostic about the role of the supply of motivated offenders [9].

PREVENTIVE MEASURES FROM CYBERCRIMES

Preventing cyber-criminals activities is not an easy task. [6] said that cyber-criminals are often difficult to identify since they committed their crimes at the very long distance from their victims. Sometimes, the country in which they live and/or have their criminal activities does not have strong criminal laws against cyber-criminality. Despite of these challenges, some measures can be taken to account as the way of combating these cyber criminals' activities as listed below.

User identification & Authentication

User identification typically includes the use of user names and passwords. However, these simple tools can be very easy for a cyber criminal to break. Passwords can be made harder to break by various techniques including requiring longer character strings, the inclusion of numbers as well as letters, making them case sensitive, and requiring that they be changed at regular intervals (e.g., monthly, annually). Password should be changed with regular interval of time and it should be alpha numeric and should be difficult to judge [7]. The use of smart cards is expected to increase in the future since it requires both the card and a personal identification number known only to the card holder. Access is impossible without both pieces.

Using network scanning programs

For large to medium enterprises, the proven Virtual Private Network (VPN) technology over WLAN, which is a practical and scalable design can be used for the security. A VPN allows users on a public or un-trusted network, like the internet or WLAN to setup a secure connection to a private network. In a wired or wireless network, the user establishes a secure VPN tunnel to the VPN server when user authorization is successful. Then all the traffic sent through the tunnel is encrypted [4].

Using open source for security

Another way of preventing cybercrimes is through the uses of Open source software. [8] wrote that; open source enables users to evaluate the security by themselves, or to hire a party of their choice to evaluate the security for them. Open source even enables several different and independent teams of people to evaluate the security of the system, removing the dependence on a single party to decide in favour of or against a certain system.

Special law Protecting Computer Users

The paper has shown that, many countries do not have any special Act

which has been established to combat computer crime activities. Though many countries have Communications Regulatory Authority (CRA), many of these regulatory authorities do not have any clear Act which protects computer users. For instance in Tanzania, The Tanzania Communications Regulatory Authority has come up with the ACT known as 'THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT, 2010' (EPOCA) but it does not consider the protection of ICT users against cybercrimes [7].

CONCLUSION

Cyber crime is indeed getting the recognition it deserves. However, it is not going to restrict that easily. In fact, it is highly likely that cyber crime and its hackers will continue developing and upgrading to stay ahead of the law. So, to make us safer we must need cyber security. As someone rightly said, "Bytes are replacing bullets in the crime world". Cyber space offers a plethora of opportunities for cyber criminals either to cause harm to innocent people, or to make a fast buck at the expense of unsuspecting citizens. We know that forensic evidence is important in normal criminal investigations. But collection and presentation of electronic evidence to prove cyber crimes have posed a challenge to investigation and prosecution agencies and the judiciary. We need a good combination of laws and technology in harmony with the laws of other countries and keeping in mind common security standards in other to help those who are vulnerable.

REFERENCES

1. Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, 1(2): 121-130.
2. Black , G. Patrick and Hawk, Kenneth R. (2010) Computer and Internet crimes, San Francisco, California [Online] available from [March 29, 2011]
3. Chang Su and Thomas J. Holt (2010) Cyber bullying in Chinese Web Forums- An examination of nature and extent, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 672–684
4. Collins, Jason D, Sainato, Vincenzo A. and Khey, David N.(2011) Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors Vol 5 Iss 1, pp 794-810
5. D. Ariz. (2000). American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc. Civ. 99-185
6. Dion, Michael (2010) Advance Fee Fraud Letters as Machiavellian/Narcissistic Narratives, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 630–642
7. Gordon, L. A. (2003). A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.
8. Issac, Biju., Mohammed, Lawan A (2007). War Driving and WLAN Security Issues - Attacks, Security Design and Remedies: The Journal of Information Systems Management, Vol. 24 Issue 4, p289-298,
9. Marion, Nancy E. (2010). The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation,, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 699–712