A SURVEY ON CYBER CRIME PERPETRATION AND PREVENTION: A REVIEW AND MODEL FOR CYBERCRIME PREVENTION

Erick K. Rotich  
Computer Science Dept Masinde Muliro University of Science and Technology, KENYA  
rotik2002@yahoo.com

Shadrack K. Metto  
Computer Science Dept Masinde Muliro University of Science and Technology, KENYA  
skmetto@yahoo.com

Lily Siele  
Dept of Mathematics and Computer Science Dept, University of Eldoret KENYA  
gimuchiri@gmail.com

Geoffrey M. Muketha  
Computer Science Dept Masinde Muliro University of Science and Technology KENYA


ABSTRACT

Threats posed to organizations by cyber crimes have increased faster than potential victims or cyber security professionals can deal with them, placing targeted organizations at considerable risk. The growth of the threat of cyber crime has outpaced that of other cyber security threats. At the moment cyber criminals are increasingly skillful at gaining unnoticed access and maintaining a relentless low profile. In this paper we review on cyber crime prevention methods. We first explore on the types of cyber crime, how it is perpetrated and how to prevent it and finally reviewed models for CyberCrime preventions. From the study we recommend a development of CyberCrime prevention Model.

Keywords: CyberCrime, Cyberstalk, Net crime, Computer crime.

INTRODUCTION

The growth of the threat of cyber crime has outpaced that of other cyber security threats. Nowadays cyber criminals are increasingly skillful at gaining unnoticed access and maintaining a relentless low profile. In the meantime, many organizations may be leaving themselves susceptible to cyber crime based on a false sense of security, using agile security tools and processes. Many fail to recognize cyber crimes in their IT environments and misallocating limited resources to minor threats.

Cyber crime may be committed irrespective of organizations trying to prevent hackers and blocking pornography. This has generated major risk exposure, including exposure to financial losses, regulatory issues, data loss, damage to brand, and loss of client and public assurance.

According to Manali (2012), Computer crimes are criminal activities, which involve the use of information technology to gain an illegal or an unauthorized access to a computer system with intent of damaging, deleting or altering computer data. Computer crimes also include the activities such as electronic frauds, misuse of devices, identity theft and data as well as system
interference. Computer crimes may not necessarily involve damage to physical property. They rather include the manipulation of confidential data and critical information. Computer crimes involve activities of software theft, wherein the privacy of the users is hampered. These criminal activities involve the breach of human and information privacy, as also the theft and illegal alteration of system critical information. The different types of computer crimes have necessitated the introduction and use of newer and more effective security measures.

Koenig, (2002) defines Cyber Crime as A criminal offense that has been created or made possible by the advent of computer technology, or a traditional crime which has been so transformed by the use of a computer that law enforcement investigators need a basic understanding of computers in order to investigate the crime. There are two distinct sub-categories: Computer Crime and Computer-related Crime.

Computer crime refers to any crime that involves a computer and a network. Moore, (2005) argues that the computer may have been used in the commission of a crime, or it may be the target as also supported by Warren et al (2002). According to Mann (2011) Netcrime refers to criminal exploitation of the Internet. Jaishankar (2011) defines cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones such as SMS or MMS. Such crimes may threaten a nation’s security and financial health.

Govil (2007) regards Cyber crime as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cyber crimes describe criminal activity in which the computer or network is a necessary part of the crime. From this definition it is evident that the computer is the key source of cyber crime. Cyber crime is increasing in the list of internet- Aided offenses. This crime is almost overtaking street crimes, because street crime is almost contained and may soon be regarded as the thing of the past. Street crimes do take place but computer crime is more expedient. Cyber crime has demonstrated to be accurate, easy, and reliable; detection is difficult and hence it has become hard to prevent it.

Cyber crimes can be principally divided into three major categories, Cyber crimes against persons, Cyber crimes against property, Cyber crimes against government. All these Cyber crime categories affect us in one way or another. In this paper we explore on the types of Cyber crime, ways in which cyber crime is perpetrated and some prevention methods.

**CYBERCRIME**

Computer crime is where a perpetrator uses special knowledge about computer technology. Cyber crime on the other hand, is where a perpetrator uses special knowledge of cyberspace. CyberCrime are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS). Cyber
crime also may target a computer by emitting computer viruses, Denial of service attacks and attacks done through malware as argued by Indika, (2011). Computer crimes involve the unauthorized use of computer technology to manipulate critical user data. In this section we present the types of Computer Crimes.

**HACKING**

Hacking is a form of computer crime where one breaks into a computer system to achieve an unauthorized access to data or Information. The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system. The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes. Another highly dangerous computer crime is the hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities as per Oak (2012) and Sabadash (2004).

**PHISHING**

Phishing is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by disguising as a trustworthy source. Phishing is carried out through emails or by luring the users to enter personal information through fake websites. Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there as defined by Oak (2012) and Josang. et al. (2007)

**COMPUTER VIRUSES**

These are computer programs that can copy themselves to a computer and which eventually harms the computer systems on a network without the understanding of the system users. Viruses multiply to other computers through network file system, through the network, Internet or by the way of detachable devices like USB drives and Compact Disc. Computer viruses are any way, some form of malicious codes written with an aim to harm a computer system and destroy information. Scripting computer viruses is a criminal activity as virus infections can break down computer systems, in that way destroying enormous amounts of significant data as argued by Oak (2012), Kendall (2010), Germain (2009) and Rohas (2008)

**CYBER STALKING**

Cyber stalking involves torturing other individuals, false accusations, transmission of threats and damage to data and equipment, using communication technology, primarily the Internet. Cyber stalkers frequently target the users by means of chat rooms, online forums and social networking websites to collect user information and harass the users on the basis of the information gathered. Obscene emails, abusive phone calls and other such serious effects of cyber stalking have made it a type of computer crime as per Oak (2012), Sankary (2006), Rodriguez (2005) and Nagpal (2008)
IDENTITY THEFT

Identity is a severe fraud that may involve stealing money and obtaining other gains using other’s identity. In this case one behaves to be someone else by using someone else's identity as his or her own. Financial identity theft is the use of a false identity to obtain goods and services and a commercial identity theft is using of someone else’s business name or credit card details for commercial purposes. Identity cloning is the use of another user's information to pose as a false user. Identity theft makes illegal migration, terrorism and blackmail to be possible as described by Hamilton, (2010) and Stroup (2012).

CYBER BULLYING

Cyber bullying is the use of cell phones, instant messaging, e-mail, chat rooms or social networking sites such as Facebook and Twitter to harass or threaten or coerce others. Children who have more and more early access to internet technologies eventually resort to cyber bullying. A bully can hide behind an electronic veil, disguising his or her true identity which makes it difficult to trace the source and encourages bullies to behave more uncompromisingly than they would on a face-to-face scenario as stated by TechTarget (2008), Dunn (2009) and Harmon (2004).

MALWARE

Malware refers to viruses, Trojans worms and other software that gets onto your computer without you being aware of them. Justin (2010) and Brenner (2009) say that those who write this software find it amusing they exploit security flaws just to find out they can spread. Malware pretend to be genuine software and may ask for money. Some malware when they attack successfully will require money to remove from the computer. This is also supported by CCRC (2005).

SPAM

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products. Spam costs the sender very little to send most of the costs are paid for by the recipient or the carriers rather than by the sender. Spam is an Electronic junk mail or junk newsgroup postings which are defined as any unsolicited e-mail. Specifically spam is generally e-mail advertising for some product sent to a mailing list or newsgroup as argued by Justin (2010). Spam is an endless repetition of worthless text that waste people's time with unwanted e-mail and consumes a lot of network bandwidth. Many organizations and/or individuals are fighting spam with a variety of techniques. Since the Internet is public, it is hard to prevent it, so is it to prevent junk mail. Nevertheless, there exist some online services who have instituted policies to prevent spammers from spamming their subscribers this is also supported by Kunz & Wilson (2004).
CHILD PORNOGRAPHY

Child pornography is any visual depiction, photograph, film, video, picture, or computer or computer-generated image or picture, which can be produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of the visual depiction involves the use of a minor engaging in sexually explicit conduct or the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct or the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct this is argued by Wolak, et. al, (2005), Carr, (2003) and Akdeniz (2003).

CYBER CRIME PERPETRATION METHODS

In this section we discuss cyber crime perpetration methods.

THEFT OF INFORMATION SERVICES

Here the perpetrators gain access to the PBX board of an organization, and make their own calls or sell call time to third parties this is said by Venkatraman (2010), In theft of services, people use a variety of techniques to obtain services without paying for them. In all forms, a person is obtaining services without providing the service provider or the person who is paying for those services with compensation in exchange. Theft of services can be seen with utilities like phones, electricity, water, cable, and Internet. Theft of services happens when people tamper with devices which are used for metering with intend to pay less, or use devices which make them bypass metering altogether and to get services for free. A common theft of services which became a problem in some areas of the world in the 2000s was theft of wireless Internet services, where people bypassed router security to access a wireless access point for which they were not paying for.

COMMUNICATIONS AS AN AUXILIARY FOR CRIMINAL CONSPIRACIES

Communications as an auxiliary for criminal conspiracies involves use of information systems to further criminal activities such as being used in gambling, drug trafficking, money laundering and weapons business as per Venkatraman (2010)

TELECOMMUNICATIONS PIRACY

Digital technology allows perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. Venkatraman (2010) argues that this has produced the temptation to reproduce copyrighted material either for personal use or for sale at a lower price. Emerging technologies in money transfer systems has made it easier to conceal the origin and destination of funds transfer. Thus money laundering comes to the living room, woda (2006) asserts that money laundering is an offence committed by some individuals locally and intentionally placed that signifies the conversion and transfer of assets of an illicit origin. The objective of this action consists of disguising the true origin, location, nature, disposition, movements and transfer of
assets that are derived from illegal activities. Participation, support or facilitation of the realization of illegal activities, such as transfer of money of illicit origin to several banks accounts and afterwards converted into legal financial products.

ELECTRONIC VANDALISM AND TERRORISM

Lejk (2006) argues that Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents. Kolo (2009) and Venkatraman (2010) define vandalism as deliberately destroying or damaging property of another. Thus computer vandalism may be any kind of physical harm done to the computer of any person. Such acts may be theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

SALES AND INVESTMENT FRAUD

Online auction comes with several activities which constitute fraudulent behaviors. According to Venkatraman (2010) Sales and investment Fraud include:

i. Non-delivery- Bidding for no item or seller doesn’t want to sell the item.
ii. Misrepresentation- The seller deceives the buyer as to the true value of the item.
iii. Non-payment- The buyer places the highest bid to win the auction but doesn’t pay for merchandise.
iv. Triangulation- The buyer buys the merchandise using stolen identities and credit card numbers.
v. Fee stacking- The seller adds separate charges for postage, handling, and shipping making the buyer pay more than anticipated.
vi. Black-market goods- The goods are delivered without a box, warranty, or instructions.
vii. Multiple bidding- A buyer places multiple bids (some high and some low) using different aliases. The multiple high bids cause the price to escalate, and scares off other potential buyers from bidding. Then, in the last few minutes of the auction the same buyer withdraws their high bids, only to purchase the item with their lowest bid.

ILLEGAL INTERCEPTION OF INFORMATION

Improvements in telecommunications and data transfer over the Internet have resulted in better speed and capacity but this as introduced greater vulnerability. It is now easier for unauthorized people to gain access to sensitive information. Electromagnetic signals that are emitted by a computer can now be intercepted where cables act as broadcast antennas. To make matters worse there no existing laws to prevent the monitoring of remote signals from a computer. Under such circumstances information is more and more vulnerable to unauthorized users as per Venkatraman (2010).
LOGIC BOMB

This is an event dependent program. This implies that this program is created to do something only when a certain event occurs (e.g. the Chernobyl virus).

Logic bomb is a piece of computer code that executes a malicious task, such as clearing a hard drive or deleting specific files, when it is triggered by a specific event. It is secretly inserted into the code of a computer's existing software, where it lies dormant until that event occurs. This event might be a positive trigger, such as a specific date and time or the removal of an employee's name from the salary database; or it might be a negative trigger, such as a particular employee failing to input a command by a certain time meaning he or she is probably not at the company anymore.

A logic bomb doesn't have much use outside of targeting a specific computer or network, and IT employees are usually the only ones with the access and know-how to implement them according to Layton (2012).

A logic bomb which is called slag code is a programming code, inserted secretly or deliberately, that is designed to execute (or explode) under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. It is in effect a delayed-action computer virus or Trojan horse. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects as said by TechTarget (2012) and Kolo (2009).

INTERNET TIME THEFT

Some an unauthorized person may use Internet time paid for by someone else. Nagpal (2008) connotes the usage by an unauthorized person of the Internet hours paid for by another person.

SALAMI ATTACK

Salami attack is used to commit financial crimes. Here the idea is to make the modification so small that in a single case it would go unnoticed. A bank employee, for instance, can deduct five cent US dollars from every customer's account. Customers account holders may not notice this little change but the bank staff will make large amounts of Money as according to Nagpal (2008).

In the salami technique, criminals steal money or resources a bit at a time. It refers to slicing the data thinly. A programmer can create salami attack by modifying arithmetic routines, such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary two or three kept for financial records. For example, a programmer arranges to collect money in fractions of pennies in a separate account; a sizable fund can grow with no warning to the financial institution as according to Kabay (2002).
DATA DIDDLING

This kind of attack involves altering the raw data before it is processed by a system and re-altering it after processing as said by Nagpal, 2008.

Kabay, (2008) argues that data diddling is associated with electronic data processing where illegal or unauthorized data is altered. The changes can happen before and during data input or before output.

E-MAIL BOMBING

Nagpal (2008) explains this as sending a large number of mails to the victim resulting in the victims mail account (in case of individual) or server (in case of corporations) crashing. Email bombing is a form of denial of service attack that floods an inbox and mail server with messages. So many messages are sent that eventually the systems may be overloaded and they will stop working. Kolo (2009) explains email bombing that it may be coordinated in two ways namely:

- Sending large numbers of email directly, often using multiple accounts and scattering the emails out over many accounts that makes it harder to pin down the source of the attack. A virus can be written to hijack email accounts held by other people and use them to bomb the target.
- List bombing where the subject is signed up for large numbers of mailing lists.

VIRUS/WORM ATTACK

A virus is a program that is able to attach itself to one or more files or a system and then circulates to other files and to other computers via a network. Standler (2002) explains it as being able to affect computers by either altering or deleting data from it. Worms do not interfere with data but multiply until they fill all the memory space on the computer.

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on the victim’s computer, use the victim’s e-mail program to spread itself to other computers, or even erase everything on the victim’s hard Disk. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Viruses can also spread through downloads on the Internet. They can be hidden in illicit software or other files or programs.

Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer’s memory.

CYBER STALKING

This involves following a person on the Internet and causing harassment as explained by Standler, (2002), Nagpal (2008) and Venkatraman (2010).
CYBERCRIME PREVENTION METHODS

This section provides common cyber crime prevention methods.

FIREWALLS

These are programs, which protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people who the user permits. A firewall works directly with a router program, which examines each network packet to determine whether to forward it toward its destination. A firewall works with a proxy server that makes network requests on behalf of workstation users.

A firewall if it is a program is installed in a particularly designated computer separate from the rest of the network so that no incoming request can penetrate directly at private network resources. A number of firewall screening methods exist. A simple one is to screen requests to make sure they come from acceptable domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates as explained online by howstuffworks.com.

There are two major types of firewalls which are network firewalls and host-based firewalls. Network firewalls, for example, the software-based Microsoft’s Internet Security and Acceleration (ISA) Server or the hardware-based Nortel Networks Alteon Switched firewall System, protect the perimeter of a network by watching traffic that enters and leaves. Host-based firewalls, such as Internet Connection Firewall (ICF—included with Windows XP and Windows Server 2003), protect an individual computer regardless of the network it’s connected to source.

FREQUENT PASSWORD CHANGING

With the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first thing to do.

If someone had hacked your password and has been accessing your account without your knowledge will immediately be shut out once your password is changed. There is need to schedule the change of password in a period like six months. This is necessary because some people can sell an old computer and forget to erase passwords they may have saved for dialing in or for accessing their email.

If you change your password at least every three months, hackers who may be trying to crack your password using brute force essentially need to start over again because the changed password could now be possessing new pattern which they might have already tried and rejected.

It is good idea to force a password change because it discourages users from using the same password on multiple accounts. Changing password frequently poses the danger of picking on
poor passwords. This makes the situation even worse, because it now allows attacks that would have otherwise not been possible explained by Ingham (2002) and Tyson (2012).

SAFE SURFING

This is a practice, which should be pursued by all users on a network. Secure surfing involves keeping ones e-mail address confidential, not chatting on open systems, which do not have adequate defense techniques and visiting secure sites. Accept data from only known users, be cautious when downloading and more so from known sites to reduce cyber crime risk.

FREQUENT VIRUS CHECKS

One should frequently check his/her computer for viruses and worms. Check any external media such as floppy disks and CD ROMS for viruses before running. Computers used in business environment should use up-to-date anti-virus software. When anti-virus programs are activated they help keep computers safe from malware in two ways.

i. It can get rid of known malware – The anti-virus software scrutinizes the computer’s hard drive for known viruses and eliminates any detected malware.

ii. It avoids new malware – The anti-virus software keeps track of running computer procedures and will obstruct any suspicious computer code or files.

EMAIL FILTERS

Email filters are programs which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed. Email Filtering is one of the most readily available spam prevention techniques. There are two key forms of filtering, Content Based Filters and Bayesian Spam Filters.

Content Based Filters is broken into two main sections which are Spam Filters which are responsible for removing something on the basis of a rule previously set and Anti-filter screens which filters and sorts all received mail in form of wanted and unwanted emails, Anti-filter will keep junk mail in a separate folder, and thus averts those irritating emails from appearing in the inbox.

Bayesian Filtering calculates the likelihood of a message being spam based on its contents. It improves its filtering capability according to the mail that is grouped as spam and non-spam. Some of the issues that are taken into account are words in the body, headers, code, Links, Word pairs and Phrases.

A REVIEW OF CYBERCRIME PREVENTION MODELS

In this section we review CyberCrime prevention models.
KVIRUS PREVENTION MODEL

Wang et al. (2009) presented the Virus prevention model, which is a new technique of identifying the virus activity. Figure below shows this model.

![Diagram of Virus Prevention Model]

The process of VPM

Fig 1. Source: Askerniya Imran et al. n.d

In this model, the researchers identified the viruses, by their behavior which is very different compared to the normal software behavior. However, merely looking at code-block (signature) is easily evaded by obfuscated viruses; but it is very hard to manage them. This is a good reason to detect viruses by their program behaviors rather than their code signatures.

CYBERCRIME DETECTION MODEL

Cyber Crime is the latest and perhaps the most specialized and dynamic field in cyber laws. Some of the Cyber Crimes like network Intrusion are difficult to detect and investigate even though most of crimes against individual like cyber stalking, cyber defamation and cyber pornography can be detected and investigated through the following steps.

After receiving mail

1. Give command to computer to show full header of mail.
2. In full header find out the IP number and time of delivery of number and this IP number always is different for every mail. From this IP number we can know the Internet service provider for that system from which the mail had come from.
3. To know about Internet Service Provider from IP number, take the service of search engine like nic.com, macfvisualroute. Com, apnic.com, arin.com.
4. After opening the website of any of above mentioned search engine, feed the IP number and after some time name of ISP can be obtained.
5. After getting the name of ISP we can get the information about the sender from the ISP by giving them the IP number, date and time of sender.
6. ISP will provide the address and phone number of the system, which was used to send the mail with bad intention.
After knowing the address and phone number, a criminal can be apprehended by using conventional law enforcement methods.

**DISCUSSION**

There are several risks associated with cyber crime which result in monetary or data loss especially on online transactions. The risk of cyber crime is geared to data, information, assets, and online transactions which are continually evolving, whereas the available cyber security cannot cope with the menace. Organizations remain uninformed of their security models and no effective prevention methods against cyber criminals who seem to heavily invest part of their major profits in developing new capabilities for committing cyber crime exist.

The antivirus vendors have found it difficult to contain the amount of new malware. Cyber criminals normally exploit the resulting vulnerabilities.

The present danger is that criminals and criminally mined enterprises have hired, purchased, or otherwise acquired the ability to infiltrate systems with new penetration techniques while developing a criminal e-business network. A number of hackers have discovered that they can make more money using online crime.

Computer crime is committed using a computer and the network; therefore, computer networks may be vulnerable to many threats along many avenues of attack.

There are so many ways of preventing CyberCrime but the cyber criminals are good at bypassing the security measures that may be in place. Some of the CyberCrime are committed internally by insiders; such crimes are more costly and damaging than attacks from outside. There are several security measures that are more effective in protecting an organization from a CyberCrime.

To curb CyberCrime, there is need for businesses to conduct periodic penetration tests of their systems, implement periodic security education and awareness programs for their employees, and deliver regular communication about security from senior management.

The businesses should identify insider threats by monitoring the online activities of employees who may be discontented or have resigned; this is where recession security risks have increased among employees who have been fired or laid off.

The Virus prevention model (VPM) discussed in section 5 above identifies the viruses by their behavior. This model proves to be better than those that look at code-block (signature) which is easily evaded by obfuscated viruses and are very hard to manage them. The Process of the VPM in Fig 1 above start with a dataset which filters the Normal exe files and the Virus exe, this model can be improved by including files with different extensions like the .zip, .rar, .jpg which are known to be used by attackers to disguise virus introduction.
CONCLUSION

Information theft has led to the compromise of intellectual property, credit card information, electronic funds, identity theft, and a host of other negative consequences. Electronic theft or cyber crime affects individuals, corporations and government entities. Breaches are routinely perpetrated by, ill intended employees, ex-employees, organized crime groups, and foreign government sponsored espionage groups.

One of the ways of curbing cyber crimes by all intent and purpose is through counseling. As advised by Omoluabi (2008), parents need to monitor their children especially when they spend time out of the home. In addition, there is need for law enforcement agencies to have a tighter control of cyber café operators because they aid and assist criminals. When such cases of cyber crimes are detected, the owners of cyber cafes should be prosecuted.

This research has highlighted the importance of awareness as a tool to decrease/ prevent cyber crime. The next stage of research is to develop CyberCrime prevention process model. Our Model will enhance VPM so that the VPM process will include an additional dataset which will examine the behaviors of files with different extensions other than those with exe. The researchers will in include a module to open the said files and then subject to the VPM process.

REFERENCES


Dibu Ojerinde ,Thomas N. Kolo,2009.Cyber Crimes in e - Registration


http://searchsecurity.techtarget.com/definition/firewall retrieved on April 20, 2012


Krzysztof woda, 2006. Money laundering techniques with electronic payment systems


Pot Justin, 2010. *Five Computer Crimes & How to Protect Yourself from Them*


