Cybercrime: A threat to Network Security

Ammar Yassir and Smitha Nayak,

Department of Computing, Muscat College, Sultanate of Oman

Abstract
This research paper discusses the issue of cyber crime in detail, including the types, methods and effects of cyber crimes on a network. In addition to this, the study explores network security in a holistic context, critically reviewing the effect and role of network security in reducing attacks in information systems that are connected to the internet. As, all this adversely affects the efficiency of information security of any kind of security that exists and is used in information systems. Since hackers and other offenders in the virtual world are trying to get the most reliable secret information at minimal cost through viruses and other forms of malicious soft-wares, then the problem of information security - the desire to confuse the attacker: Service information security provides him with incorrect information; the protection of computer information is trying to maximally isolate the database from outside tampering. In other words, the Internet is a large computer network, or a chain of computers that are connected together. This connectivity allows individuals to connect to countless other computers to gather and transmit information, messages, and data. Unfortunately, this connectivity also allows criminals to communicate with other criminals and with their victims.

Keywords
Security, Network Security, Computer, Privacy, Cyber Crimes.

1. INTRODUCTION

The advent of computers and the expansion of the Internet made likely the accomplishment of large improvement in research, surgery, expertise, and communication. Unfortunately, computers and the Internet have furthermore supplied a new natural environment for crime. As Janet Reno, U.S. advocate general throughout the Clinton management, put it, "While the Internet and other data technologies are conveying tremendous advantages to humanity, they furthermore supply new possibilities for lawless individual behavior" (Dasey, Pp. 5-19).
Cybercrime is roughly characterized as committing a misdeed through the use of a computer or the Internet. The Internet has been characterized as "collectively the
myriad of computer and telecommunications amenities, encompassing gear and functioning programs, which comprise the interconnected worldwide mesh of systems that provide work the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to broadcast data of all types by cable or radio" (Internet Tax Freedom Act of 1998: 112 Stat. 2681–719). In other phrases, the Internet is a large computer mesh, or a string of connections of computers that are attached together. This connectivity permits persons to attach to countless other computers to accumulate and convey data, notes, and data. Unfortunately, this connectivity furthermore permits lawless individuals to broadcast with other lawless individuals and with their victims. Although no unanimously acknowledged delineation of cybercrime lives, a distinction is often made between a customary misdeed that is perpetrated through the use of a computer or the Internet and a misdeed that engages expressly aiming at computer technology (Richards, Pp. 21-54).
This paper provides an understanding of how network security protection can help a firm to keep its information safe from potential losses. The research builds upon extensive research and literature related to network security and protection. The paper gives a comprehensive account of some most important security tools (like firewalls) which can help companies to secure their information networks from unauthorized use. A brief account of challenges faced in Network Security Management is also provided to identify the potential areas for research.
Thesis Statement:
There are a number of adverse impacts of cyber-crime on networks, and the network security reduces them to a significant extent.
Purpose:
The purpose of the study is to determine the impact of cybercrimes on network security and to determine at what level network security is able to reduce cyber-crimes.

2. Aims and Objectives

- To determine the impact of cybercrime on networks.
- To determine the advent of cyber-crime.
- To determine the pros and corn of network security.
- To determine how network security reduces the treat of cyber-crimes.

Manuscript received February 5, 2012
Manuscript revised February 20, 2012

3. Research Design

The search will base on secondary data accumulation. The data will be pressed out from various journals, articles and books. Secondary research depicts information assembled by literature, broadcast media, publications, and other nonhuman origins. This type of research does not necessitate human fields. The research accession used is qualitative and used the case study methodology. Qualitative research is practically more immanent than quantitative one.
Methods of research in order to achieve intended tasks various theoretical and empirical methods are invoked in the master thesis. Theoretical methods of research: Historical method is applied to provide knowledge about cyber-crimes and network security. Logical methods (generalization, induction, deduction) are invoked to generalize the used literature and to draw inferences.

4. Materials and Methods

The measurements of choice for literature were relevancy to research topic and year of publishing. Both public and individual libraries, as well as online libraries, were chaffered to approach the data. Some of online databases that were accessed are SAGE, Questa, emerald, proudest and so on. Data collection establishments, for example, Gallup and AC Nielsen carry on researches on a repeated basis homing in on a wide lay of subjects. A library is an assemblage of services, resources and sources.
It is organized for the functioning of and is maintained by a public body, an organization, or even an individual. In the formal sense, a library is a collection of books. The term can mean the aggregation, the construction that homes such an assemblage, or both. Public and committed accumulations and services of process may be designated for use by individuals who prefer not to or cannot spend to purchase a huge collection, who require significant material that no person can fairly be anticipated to bear, or who demand professional help with his/her probe.

5. Research Approach

An effective strategy will be used to collect most of the information and data from various sources. The research will contain two parts, firstly “Secondary Research” in which the researcher will go through various research papers, electronic journals and database. Whereas for “Qualitative Research”, different methods that will be used to collect information from companies.

6. Data Analysis

Understanding the nature and function of cyber-crimes and network security; the qualitative descriptive mechanism is the most ideal means of collecting and analyzing data due to the flexibility, adaptiveness, and immediacy of the topic. This brings inherent biases, but another characteristic of such research is to identify and monitor these biases, thus including their influence on data collection and analysis rather than trying to eliminate them. Finally, data analysis in an interpretive qualitative research design is an inductive process. Data are richly descriptive and contribute significantly to this research.

7. Definition of Qualitative Research

Qualitative research is much more subjective as compared to quantitative research and employs very unlike methods for data accumulation. These methods are primarily interpersonal, in-depth consultations and focus groups. The nature of this type of research is explorative and open-ended. Small counts of people are questioned in-depth, and a comparatively small number of focus groups are conducted. Participants are called for to reply to general questions.

8. Consideration of Qualitative Research

Qualitative research measures consider a universal law in the hope of developing a static reality; on the other hand, qualitative research is an assumption of what the reality is a dynamic exploration. To solve the current problems of the market, it is important for retailers to adopt a more strategic approach to decision making, taking into account the great importance of intellectual property management, it does not say what is found in the process of universality, therefore, promotion and tolerance is often cited as a study of these types.

9. Result

Computer geniuses, usually in their twenties, are thrown challenges to break one or another security program, capture the passwords to remote computers and use their accounts to travel the cyberspace, enter data networks, airline reservation systems, banking, or any other "cave" more or less dangerous. Managers of all systems have tools to control that "all is well", if the processes are normal or if there is suspicious activity, a user is using to access roads which is not authorized. All movements are recorded in system files, which operators review daily (Farmer & Charles, Pp. 46). Furthermore, the network is becoming the ideal place for criminals and terrorists to carry out their actions and

activities. Hence, cybercrime and cyber terrorism have become two of the most serious threats seem to haunt Western societies. Moreover, the impact of the crimes on the victims and their measures to cope up with such crimes in the future will also be a part of the paper. This paper will also discuss the how network security is critically important in preventing the recurrence of these types of cyber-attacks in the future.

10. Discussion and Analysis

After analyzing the results of the study through qualitative analysis it can be said that computers and the Internet are now a familiar part of our lives. You may not see them often, but they are involved in some way in most of our daily activities in the business, educational institutions, and government. Without the support of any of these tools, we would be able to handle the overwhelming amount of information that seems to characterize our society. But the problem of security limits the integrity of information and computer systems. More people need to know the use of computers and the protections that are daily offered for the safe handling of information (Roland, Pp. 638-645).

Cyber warfare has been defined as the process of nation-state to introduce computers of other countries or networks to cause damage or destruction. Cyber warfare is a form of warfare that occurs on computers and the Internet, by electronic means rather than physical. Moreover, the Internet is a means of easy access, where any person, remaining anonymous, can proceed with an attack that is difficult to associate, virtually undetectable and difficult to smuggle, let alone reaching a high impact such action directly hitting the opponent (network) by surprise. The term network security refers to protection against attacks and intrusions on corporate resources by intruders who are not allowed access to these resources.

During 1997, 54 percent of American companies were attacked by hackers in their systems. The incursions of hackers caused total losses of $ 137 million that year. The Pentagon, CIA, UNICEF, the UN and other world bodies have been subjected to interference by these people who have much knowledge on the subject and a great ability to solve the obstacles they face. A hacker can take months to violate a system and increasingly sophisticated methodologies are used by the present day hackers (Ogut, Menon & Ragunathan, Pp. 14-28). A hacker enters a prohibited area to gain access to confidential or unauthorized information.

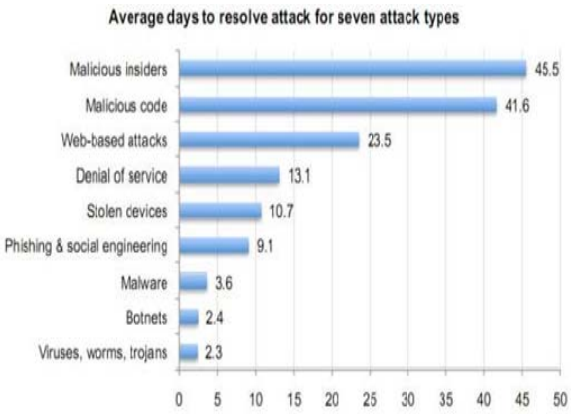
The mass media prefer to characterize them as criminals to intercept credit card codes and use them for personal gain. There are also those who intrude into airport systems producing chaos in flight schedules and aircraft. Today hacking is a prime concern of businessmen, legislators and officials.

A similar but different form of information intrusion is cracking. Crackers are people who disturb others; pirate software protected by law, destroying complex systems by transmitting powerful virus, and so on. Restless teenagers quickly learn this complex craft. They differ with hackers because they lack any kind of ideology when they do their "jobs". Instead, the main objective of hackers is not to become criminals, but "fight against an unjust system" used as a weapon system itself (Katz & Shapiro, Pp. 822-841).

Every organization should be at the forefront of change processes. Where continuous information is available, reliability and time is a key advantage. In fact, hacking is so easy that if you have an on-line and know how to send and read e-mail, you can start hacking immediately. Here you can find a guide where you can download programs especially appropriate for the hacker on Windows. Usually, these programs are free. They try to explain some easy hacker tricks that can be used without causing intentional damage (Tipton & Krause, Pp. 320-386).

The threats to the network security are not just for organizations, but can be observed all over the world in different countries and the degree to which each of them are exposed to threats. The statistics to which can be seen in the table illustrated below:

Table 1:



11. Attacks on Information: What are the Threats?

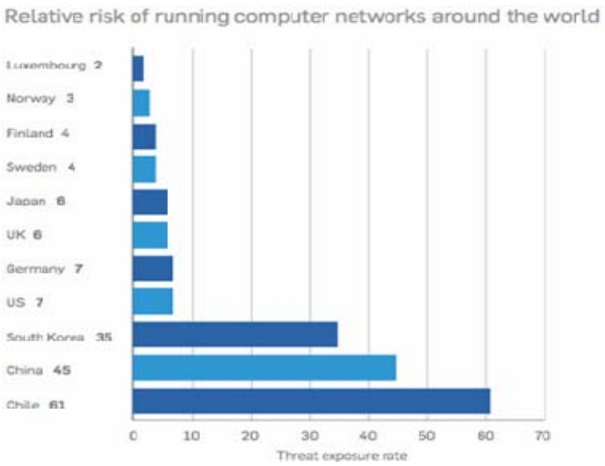
Not forgetting that the latter are always a combination of tools that have to do with technology and human resources (policies, training). Attacks can serve several purposes including fraud, extortion, data theft, revenge or simply the challenge of penetrating a system. This can be done by internal employees who abuse their access permissions, or by external attackers to remotely access or intercept network traffic.

At this stage of development of the “information society” and computer technology, hackers is no longer new. Some date back to emergence of digital networks, a good few years ago. No doubt as access to electronic communication networks became more widespread, also went by multiplying the number of those entering "illegally" to them, for different purposes. The Pirates of the cyber age considered as a sort of modern Robin Hood and demand a free and unrestricted access to electronic media (Whitman & Mattord, Pp. 205-249).

Another common attack on a computer system is the creation and distribution of malicious computer code, called “viruses”. Computer viruses are computer programs written specifically to damage other computer systems. Sometimes these malicious programs are contained within another program, known as a “Trojan horse,” and are copied by a user without his or her knowledge (Richards, Pp. 21-54).

The approximate time to resolve some categories of attacks on networks can see in the following table:

Table 2:



12. Benefits of network Security

1. Prevents unauthorized users from accessing your network.
2. Provides transparent access to Internet-enabled users.
3. Ensures that sensitive data is transferred safely by the public network.
4. Help your managers to find and fix security problems.
5. Provides a comprehensive system of warning alarms attempt to access your network.

The following table lists the most common types of Information Security Network Protection ISNP packages (Network Security Packages) in use by large organizations:

Table 3:

Name	***Description***
BlackIce	There are several levels of protection and warns us when we scanned through a sound and a flashing icon. It offers a wealth of information about the attackers and attacks following statistics, broken down by hours, days and months.
Conseal PC	It is a bit outdated and tends to disappear when there is an installation of several old files.
Tiny	It comes configured with a medium security level, suitable for normal Internet browsing. The network works fine without having to set special rules.
Protect X	Leave some open ports and others as closed. It notes from where you've connected the port. Facilitates IP registration information.
Sygate Firewall	Interface comes configured with a high level of security.
Win Route Pro	It is a proxy server. Its source addresses filtering and destination of both incoming and outgoing. It does not consume system resources and is not necessary to install an sw.
Zone Alarm	It not only detects all access from the Internet unless it gives control of the programs try to access the Internet. You can select levels of protection and block access to Internet after a certain time.
At Guard	Allows you to define rules for everything, is fast and gives you a control of what is happening. Blocks unwanted advertising has a log of date, time, URL, IP, bytes sent and received and time of all Web connections.
Esafe Desktop	Consumes many system resources, you can prohibit total or partial access to your computer.
Freedom	It is very easy to install, pass ports invisible so you can surf the Internet anonymously.
Hack tracer	You can identify the attacker, since it has a program that includes a world map with the route of the attacker's computer. Easy to install and default pass all ports invisible.
Internet Firewall 2000	Does not work on local network, you can see active connections

13. Conclusion

In conclusion, it can be said that attacks on machines connected to the Internet have increased by 260% since 1994, with an estimated loss of 1,290 million dollars annually in the U.S. In the era of information, ideas, data and files on your network are probably more valuable than your entire company. Think about your customer lists and records of shareholders, trading and marketing materials, marketing strategies and product design, the loss of which could mean the significant loss for your firm. With advances in technology, no one is safe from an attack by "hackers. Currently it is relatively easy to gain control of a machine on the Internet that has not been adequately protected. Companies invest a significant portion of their money in protecting their information, since the loss of irreplaceable data is a real threat to their business. The technology boom in the development of networks, digital communications and

advances in software technology allowed the birth of a virtual world whose ultimate expression is the Internet.
Today, for the implementation of effective measures for protecting information requires not only protection of information networks and mechanisms for a model of network security and implementation of a systematic approach or a set of data protection - a complex of interrelated measures, described by the definition of "protected information".

References

[1] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press, 2011: Pp. 5-19.
[2] Farmer, Dan. & Charles, Mann C. Surveillance nation. Technology Review; Vol. 106, No. 4, 2003: Pp. 46.
[3] Harrison, A. Privacy group critical of release of carnivore data. Computerworld; Vol. 34, No. 41, 2006: Pp. 24
[4] Internet Tax Freedom Act of 1998: 112 Stat. 2681–2719. Retrieved from: (http://www.cbo.gov/doc.cfm?index=608&type=0). Accessed on : 29th January, 2012.
[5] Katz, Mira L. & Shapiro, Carl. Technology Adoption in the Presence of Network Externalities. Journal of Political Economy; Vol. 94, No.4, 1986: Pp. 822-841.
[6] Ogut, Hulisi. Menon, Nirup. & Ragunathan, Srinivasia. Cyber Insurance and IT Security Investment: Impact of Independent Risk. Proceedings of the Workshop on the Economics of Information Security (WEIS), Cambridge, MA: Harvard University, 2005: Pp. 14-28.
[7] Richards, James. Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators. Boca Raton, FL: CRC Press, 1999: Pp. 21-54.
[8] Roland, Sarah E. The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?. Suffolk University Law Review; Vol. 35, 2001: Pp. 638-45.
[9] Tipton, Harold F. & Krause, Micki. Information security management handbook (5th ed.). London: Taylor & Francis e-Library, 2005: Pp. 320-386.
[10] Whitman, Michael E. & Mattord, Herbert J. Principles of information security (2nd ed.). Boston: Thomson Course Technology, 2005: Pp. 205-249.

Ammar Yassir received the B.Sc. degree with Honors in Computer Science in the year 2002 from Future University, Sudan and Master in Business Administration and Information Technology degree from Sikkim Manipal University, India in 2006 and currently a Ph.D. candidate in Information Technology, CMJ University, Shillong, India. He is now lecturer at Muscat College, Sultanate of Oman. He has published an international paper in IJCSNS.

Smitha Nayak received the B.Sc. degree in Physics in 1998 from Mumbai University, India and Master of Computer Application degree from Visweshwaraiya Technological University, India in 2001 and currently a Ph.D. candidate in Information Technology, CMJ University, Shillong, India. She is now lecturer at Muscat College, Sultanate of Oman. She has published an international paper in IJCSNS.