Cyber crime and internet security essay sample

Law, Security

Title: To investigate the various forms of cyber crime and internet security and privacy threats in reference to developing countries.

1. 0 Introduction.

Cyber crime, security and Privacy have become synonymous with internet use. This scenario although common all over the world is more rampant and pronounced in the developing world where by many institutions do not have the necessary resources required to effectively fight the vice. Rarely can any one think of doing online transactions without first worrying about the twin issues of security, and privacy.

Internet security is particularly a tricky and complex phenomenon because of the lack of universality in implementation of various security policies and acts. Secondly, the advent of internet as well as its ever rising relevancy and popularity has caught many stakeholders including governments, software companies as well as regulatory agencies by surprise. At first few would imagine that internet could be used negatively.

However this has in recent times become a reality and cyber crime can authoritatively be termed as one of the most dangerous crimes acing globalization efforts and the business world in particular. What makes cyber crime particularly dangerous and therefore puts it in a class of its own is the fact that, it can cover a wide area in terms of geographical scope. In terms of efficiency, it is very fast as well as reliable. Thirdly it takes and requires enormous resources to detect. Only the most sophisticated software, expertise and technology can detect cyber crime, leave alone thwarting it.

1. 1 Rationale

The research on cyber crime could not have been carried out at a more appropriate time. This research is timely because the concern for internet security has never been so central to online transactions. Therefore this is the right time for this study as the findings will fill a gap in the internet security problem.

1. 2 The research questions.

Although the objective of the research is to investigate the different forms of cyber crime as well as security and privacy breaches over internet, the research shall also aim to contribute to the better understanding of how the different forms of cyber crimes are perpetrated as well as how they can be prevented. To be able to cover the research problem wholly and in depth, the research questions below will guide the study. After the research is completed as provided for in the Gantt chart, it is hoped that, every single of the following questions shall be answered comprehensively.

- What can be done to overcome the problem of security and privacy?
- What resources are required in the fight against cyber crime?
- Who are the players and what is each of the stakeholders' specific roles?
- Is the war against cyber crime lost or is there a still a good chance of success?
- What are the effects of cyber crime and the issue of security and privacy on national economies of developing countries?

This research shall seek and endeavor to provide answers to the above problems.

1. 3 Limitations of the study

The research is faced by some limitations key of which is the unavailability of similar research studies carried out on the same problem with developing countries in mind. However attempts will be made to apply the context of developed countries to the developing countries although this will be done carefully so as to avoid misguiding the consumers of the research findings. It is anticipated that, many of the respondents may not be willing to bring forth honest answers due to privacy concerns. This is a limitation in that; respondents may fail to disclose crucial information to the researcher.

1. 4 Research Benefits

This research hopes to benefit the developing countries to better understand the complex issues of cyber crime, internet security and internet privacy. By doing so, the researcher hopes that, that will prevent the developing countries from losing valuable resources to internet attackers ad probably save the money for other social programmes. The research also will contribute a wealth of literature to the existing body of knowledge of internet security. The research will also be beneficial to the business community which is likely to become more protected from cyber crime if recommendations of the report will be adhered to.

- Literature Review
    - Cyber crime

Cyber crime is not very easy to deal with because data and information on the extent of the crime is not available. In most cases only some countries especially America, European and Asian countries seem to gather and store cyber crime related data. This has made the war against cyber crime a challenge (Robertson, 1999). This situation is considered a disadvantage in the fight against cyber crime in the sense that, it is often difficult and in some cases impossible to fight a crime whose causes and manifestations are not clear.

However as (Smith, Byron 1996), notes, there is no need for pessimism as already major international companies have adjusted their security in terms of internet safety and given privacy and security a priority in terms of budget allocations. Contrary to the above statement, the amount of money and companies reported to be involved in cyber crimes have continued to increases significantly (Jeff, 2000).

This clearly points to a problem worthy investigating. Thanks to advanced security software, the willingness of companies and government security agencies to share information, the threat of cyber crime is a battle that can be won. There are numerous categories of cyber crimes all of which will have a bearing to this research. Due to the fact that, such portend serious threats to internet security and privacy, such are discussed in the following sections in depth. As noted by (Jeff, 2000), the reasons for internet attacks differs significantly just as the repercussions do.

Hacking refers to the access to and use of a program to access another program or system to which the attacker is not authorized (McClure,

Scambray, & Kurtz, 2003). Although the term hacking is not a very old terminology, it has gained ground amongst the internet users. According to (John, 2000), hacking has become one of the greatest security threats to e-business. Reasons for hacking have been cited as retaliation, as well as in some cases politically motivated reasons (McClure, Scambray, & Kurtz, 2003). Hacking could also involve physical vandalism of a system's physical components.

- Use of codes.

Use of malicious codes has become a common security breach in the recent years (Northcutt, & Novak, 2000). The attackers in this case have a mission of inflicting heavy financial losses to their victims. Usually the attacks involve the use of worms which victims may mistake for Microsoft security updates (Piller, 1998). These programs once infiltrated into a victim's computer network end up deleting important files something which results into loss of valuable data.

- Fraud

Fraud involves defrauding online and as more and more people turn to payment online, the threat of fraud over the internet is continually becoming very real. According to (Merkow, & Mark, 2002), victims of internet fraud are enticed by the promise of high returns for investment. Therefore, they commit themselves into paying huge sums of money through the internet. This form of cyber crime has financial motives as the key reason for the attacks.

- Vulnerability

Vulnerability refers to a form of cyber crime whereby attackers capitalize on weaknesses of the simple network management protocol (Schneider, 2000). Such vulnerability exposes a company's intranet to attackers. Although (Flynn, 2001), notes that this is not a very common type of cyber crime, attackers could cause major damages where they to infiltrate a company's system using the vulnerability.

- Denial of service

This is a form of a security breach in which an attacker blocks the authentic persons from accessing their own system (Escamilla, 1998). Although it is the easiest form of cyber crime to detect (Dieter, 1999), it usually has far reaching effects once executed as it leads to failure of systems to function normally leading to interruptions of business. According to (Plunkett, 2000), such attacks are designed to either put victims out of business by interfering with their web pages or preventing end users from accessing and communicating with the target victim and are common in developing countries.

3. 0 Methodology

3. 1 Research design

The research will utilize quantitative and qualitative approaches as well as suitable data collection instruments such as questionnaires, oral interviews including structured and semi structured interviews besides telephone conversations. Data shall be collected from a random sample of 180 respondents working in a total of 7 countries all from developing countries.

3. 2 Analysis.

Data analysis for both the qualitative and quantitative data garnered in the data collection will be analyzed using SPSS in order to arrive at findings. The findings shall be represented in form of graphs, bar-charts, and pie-charts as well as easy to interpret tables.

3. 3 Ethical considerations

Participation in the research will be on voluntary basis and since selection of the respondents will be done by random selection, it is hoped that, the issue of denial of participation does not arise. The research shall only restrict the questions to thse which does not lead respondents to give personal or confidential information thius exposing themselves to possible dangers. Also, the research shall take necessary precaution measures so as not to expose respondents to physical or psychological harm.

4. 0 Conclusion.

Ecommerce has changed the concept of business and helped overcome geographical as well as other challenges in business, but as to whether it shall over-come the security and privacy threats is another case. As challenges emerge, solutions for such are bound to be found and therefore stakeholders need to find long-lasting solutions to the problem of cyber crime.

5. 0 APENDIX A REFERENCES:

Dieter, G,. Computer Security. Wiley & Sons. New York, NY, 1999.

Escamilla, T. Intrusion Detection: Network Security Beyond the Firewall. John Wiley &

Sons, New York, NY, 1998.

Flynn, N. The E-Policy Handbook: Designing and Implementing Effective E-Mail,

Internet and Software Policies. New York: AMACOM, 2001.

Jeff, S, . Windows 2000 Security Handbook. Que, Indianapolis. 2000.

John, H, . Windows 2000 Security Technical Reference. Microsoft Press, Redmond, WA,

Magid, Lawrence, J. High-Speed Internet Access Gets Cheaper, Thanks To Technology,

Los Angeles Times, 09/23/98, P8.

McClure, S., Scambray, J. Kurtz, G. Hacking Exposed: Network Security

Secrets and Solutions, 4th ed. McGraw-Hill, 2003.

Merkow, Mark, S. The E-privacy Imperative: Protect your Company’s survival in the

Electronic Age. New York, AMACOM, 2002.

Northcutt, S,. Novak, J,. Network Intrusion Detection, 2nd Ed. New Riders. Indianapolis.

Piller, C. Lycos. To Add Wired Digital To Portal Network, Los Angeles Times, 10/07/98, P13.

Plunkett, J. Plunkett’s E-Commerce & Internet Business Almanac. Houston, TX:

Plunkett Research, 2000.

Robertson, R. Small Business – Legislation Prepares To Click On Growing Internet

Problems. Australian Financial Review 13/07/1999.

Schneider, B. Secrets and Lies: Digital Security in a Networked World. New York.

1. Wiley, 2000.

Smith, Byron, Internet Providers Report Small Business Reluctance, ABIX – Australasian

Business Intelligence Business, 09/02/96, P18-21.