Risk of Cyber Attacks in the Network Systems of a State University in Eastern Visayas, Philippines: A Case Study

Lowell A. Quisumbing

Leyte Normal University, Tacloban City, Leyte Philippines

Abstract— *Computer network security plays a vital role in the information and communication technology (ICT) environment. This study investigates the status of the existing network security, potential risks, and the possible solutions to the existing network problems. The descriptive research design was used using a survey questionnaire as its main instrument in the conduct of the study. Findings reveal that the current status of the network security of the State University needs improvement as it handles complex information and is important in the university's day-to-day transactions. The university needs to undergo intensive evaluation and system analyses to ensure that their operation will not be hampered by malicious software or cyber hackers.*

Keywords— Network Security, Cyber Attacks, State University, Information Systems, Security Status.

I. INTRODUCTION

The influx of Local Area Network (LANs) and Wide Area Networks (WANs) paved the way for information technology based systems. Over the past decade, organizations have sought to become more efficient and productive by adopting information and communication technologies (Baker and Wallace, 2007). At present, almost every aspect of a business is supported by or based on Information Technology (IT). IT capability is critical for a firm to realize business value and sustain competitive advantage (Lu and Ramamurthy, 2011). Today, the IT industry and the internet is one of the most dynamic entities in the global economy. Governments use the Internet to provide information to their citizens and to replace manual methods of collecting information and providing government services (Lipson, H. F, 2002).

Due to the increasing demand for IT based systems, the integration of Network Information Systems (NIS) to IT-based systems was implemented. But, while companies and educational institutions are being pampered with the advantages of using IT and the Internet, there is a major factor most often overlooked, the issue of protecting the organizational assets from people or individuals who have malicious intentions against it. According to (Leeson and Coyne, 2005), in 2003, hacker-created computer viruses alone cost businesses $55 billion nearly double the damage they inflicted in 2002 (SecurityStats.com, 2004). In 2000 the total cost of all hack attacks to the world economy was estimated at a staggering $1.5 trillion (PricewaterhouseCoopers, 2000). In a 2004 survey of American companies and government agencies conducted by the Computer Security Institute, over half of respondents indicated a computer security breach in the past 12 months and 100 percent of respondents indicated a Web site related incident over the same period (CSI, 2004).

In the Philippines, cyber security attacks also make headlines. April 2012 revealed an unexpected cyber conflict between Philippine and China. Hackers who identified themselves as Chinese attacked the University of the Philippines. In that circumstance they defaced the UP website (up.edu.ph) with a map, labeled with Chinese characters, showing the Scarborough Shoal. The next day, Filipino netizens affiliated with 'Anonymous Philippines' retaliated against selected PRC websites, defacing them in turn (Gomez, 2013). The Cyber security attacks that are prevalent to date are interruption, interception, modification and fabrication. Interruption is defined as an attack against availability of services like Denial of service attacks (DOS) taking down the servers of websites. Interception attack works by gaining unauthorized access to a system using malicious software (malwares) such as trojans, virus and worms. Modification aims to modify information exchanged between parties and fabrication commonly known as counterfeiting, is mimicking or impersonating information to gain access to data(Cola, J., 2011).

To maintain their competitiveness, enterprises should safeguard their information and try to eliminate the risk of information being compromised or reduce this risk to an acceptable level (Ou Yang and Yu-Ping, 2009). It is a fact that organizations using computers in a network and the Internet face the threat of hacking from individuals within or outside of the organization. Furthermore, information systems of Cyberspace offer attractive targets (Farn, Lin and Lo, 2008).

With this scenario, it is imperative that every organization should monitor its systems for possible intrusions and unauthorized entries. Organizations should understand that the only secure system is the system which never connects to a network and never installs software. This of course is impossible in today's computer infrastructures which places an importance in connectivity (Darmawan, Chong, et.al., 2009).

The purpose of this study is to assess the integrity of the State University network security and establish a reference for future network security plan. The existing network information system, potential threats, network security status and security guideline are the predictors in creating a proposed solution for the schools network information system. To evaluate the stability of a network, (Canavan, 2001; Brenton and Hunt, 2001; Stallings, 2006) supports the idea that we have to look at the existing threats, vulnerabilities and attacks.

This study is conceived on the idea that identifying the network security status and requirements will be beneficial to the school. It will help them identify weaknesses in order to formulate good and effective procedures that will help the sustainability and smooth operation of their networks. It is in the researcher best interest to provide a more heightened security awareness on the people who supervise and maintain these network systems.

II. FRAMEWORK

The first stage of the theory of Network security situation awareness model (NSAM) states that the model of current network security situation evaluation can be proven by the degree of the threats of the various network services that have experienced attacks (Jibao, L., Huiqiang, W., & Liang, Z., 2006).

The theory is applicable to this study because in order to obtain credible data or reference for assessing the current network security status of the institution, a careful examination of the present network information system threats and the attacks that were encountered if there are any, should be undertaken. The level of threats and attacks suggests whether or not your organization is a focus of interest or if people perceive it to be housing valuable asset, in essence it is a potential target (Hunt and Brenton, 2001).

Another significant theory used in this study is the Network security situation evaluation (NSSE) framework which suggests that the evaluation on asset, vulnerability and threat can be comprehensively processed to obtain the security situation evaluation of the whole network (Chundong and YuKey, 2014).

The NSSE theory also relates to this study because the integrity of the network can only be determined by fully looking on to the weaknesses, strengths and inherent qualities of the network such as its policies and procedures and the responses it will implement in case of an attack. Only by careful analysis of these factors can we determine what is needed by the university and when it is needed. In this regard the researcher looks into the current network security resources, potential threats, and risks of the respondent institution as stated in the NSAM and NSSE model.

III. RESEARCH OBJECTIVES

This study aims to determine the network security status and requirements of the Information Systems of a State University. Specifically, these attempts to answer the following questions:

1. What is the current network security status and requirement in the network Information Systems of the university?
2. Are there potential risks, threats and vulnerabilities of the network Information Systems in the university as perceived by network personnel and administrators?
3. Are the current Network Security policies and procedures of the university reliable and effective?
4. What input can be deduced to improve the security systems of networks and information systems in the university?

IV. METHODOLOGY

4.1 Design

This study utilized the Descriptive survey method. The researcher desired to know the actual status and other characteristics of the network security of the university as perceived by the Management Information System (MIS) unit in the University for the period of SY.2014-2015.

4.2 Subject

The Administrator and staff of the Management Information System (MIS) Department of the University comprised of seven (7) personnel who maintain and oversee the operation of the Network Information System (NIS) are the respondents of this study.

4. 3 Instrument

A questionnaire consisting of five parts was the main research instrument used in this study. The questionnaire was divided into the following areas: Personal Data, Existing Network Information System Assessment, Potential Threat Assessment, Security Status Assessment, and Security Guidelines.

4.4 Procedure

In order to obtain successful results of the study, the researcher sought first the approval of the respondents after which, planning and designing of the procedure for data gathering was devised. First, the conduct of interview and observation of the respondents in the

network environment was initiated, the researcher asked about network policies, procedures, operational task and the extent of compliance to security guidelines. Then, the actual data that was obtained from the interview and observation were transcribed, classified and examined. The data was utilized for drafting the questionnaire. The survey-questionnaire was revised to fit the requirements of the study and finalized before the fielding of the instrument. The second step was the collection of the survey data looking into the relevance of data for the study. Finally, the data was tabulated and the results analyzed.

4.5 The Statistical Analysis of Data

The results obtained from the survey were tallied, tabulated, summarized and analyzed. Descriptive Statistics like Simple frequency counts, percentages, and means were used as the preliminary consideration for the analysis of the data. Microsoft Excel was used to tabulate and analyze the results.

In the assessment of existing NIS and the potential threat assessment, the following scale was used:

Rating Scale	Qualitative Description
5	Very much applicable
4	Much applicable
3	Moderately applicable
2	Applicable
1	Not applicable

Below is the qualitative description of existing NIS and the potential threat assessment with an interval of 0.8 to have an equal distribution of the rating scale:

Limits of Scale	Qualitative Description
4.21 – 5.0	Very much applicable
3.41 – 4.2	Much applicable
2.61 – 3.4	Moderately applicable
1.81 – 2.6	Applicable
1.0 – 1.8	Not applicable

The security status assessment made use of the following scale:

Rating Scale	Qualitative Description
5	Excellent
4	Very satisfactory
3	Satisfactory
2	Fair
1	Poor

Below is the qualitative description of the security status assessment with an interval of 0.8 to have an equal distribution of the rating scale:

Rating Scale	Qualitative Description
4.21 – 5.0	Excellent
3.41 – 4.2	Very satisfactory
2.61 – 3.4	Satisfactory
1.81 – 2.6	Fair
1.0 – 1.8	Poor

For the alternative solutions, the scale below was used by the researcher:

Rating Scale	Qualitative Description
5	Very much needed
4	Much needed
3	Moderately needed
2	Needed
1	Not needed

Below is the qualitative description of the alternative solutions with an interval of 0.8 to have an equal distribution of the rating scale:

Rating Scale	Qualitative Description
4.21 – 5.0	Very much needed
3.41 – 4.2	Much needed
2.61 – 3.4	Moderately needed
1.81 – 2.6	Needed
1.0 – 1.8	Not needed

V. RESULTS AND DISCUSSION

Table 1.Existing Network Information System

Network Characteristics	LNU	Qualitative description
The NIS has been in full operation for more than 5 years.	3.57	Much applicable
The NIS is composed of two or more laboratories.	4.57	Very much applicable
There are more than fifty computers connected to the NIS.	4.57	Very much applicable
The NIS is a LAN (Local Area Network).	4.86	Very much applicable
The NIS is a WAN (Wide Area Network).	2.57	Moderately Applicable
The NIS has Internet access.	4.86	Very much applicable
The NIS houses vital and important assets.	4.57	Very much applicable
The NIS is equipped with new and modern communications facilities such as modems, routers, switch, workstations and servers.	3.71	Much Applicable
The computers in the NIS are always checked and updated.	3.29	Moderately Applicable
The NIS is well funded in terms of maintenance and operability.	3.71	Much Applicable
The NIS uses new and sophisticated programs for smooth operation.	3.43	Much Applicable
The NIS human resource is sufficient to its needs.	3.29	Moderately Applicable
The NIS is being maintained by persons who are computer experts and computer literate.	4	Much Applicable
TOTALMEAN	3.92	**Much Applicable**

The table shown above (table 1) illustrate the existing network information system in the university with a qualitative result of *Much Applicable* having a total mean of 3.92. It gives us a clear idea of the hardware, software and other resources together with the assets that are present within the NIS of the University. Majority of the items rated Very Much Applicable and Much Applicable. This implies that the respondent has a higher level of knowledge on the NIS assets and its contribution to the network. Furthermore, it gives us a strong justification that the respondents pay more importance on the majority of the network resources as part of their day to day operations leading to more productivity and efficiency. However, it was also found out that there is a need to look into some areas that needs improvements. Like on the functions of the Network Information System (NIS) as a WAN, the addition of human resources to the NIS and the frequency of checking and updating the computers in the NIS. There should be no room for complacency. Complacency in the network security industry can be cited as the cause of many major intrusions and hacking strikes.

Table 2.Potential Threat Assessment

Potential threats and risks	LNU	Qualitative description
The NIS can be remotely accessed from any location.	3.29	Moderately Applicable
The NIS offers a public networking service such as serving as host or server over the Internet.	3.57	Much Applicable
There are users outside the networking staff who have been granted root or administrator privileges.	3	Moderately Applicable
User's are allowed to share a common log-on names such as guest.	2.14	Applicable
Portions of the network are electronically accessible by the public.	3.86	Much Applicable
A portion of the school or university deals with financial or monetary information.	3.29	Moderately Applicable
News stories about the school appear regularly in newspaper, magazine or website	3.14	Moderately applicable
TOTALMEAN	3.18	**Moderately Applicable**

Table 2.Shows the potential threat or the risk of a cyber attack that may result to the obliteration of information available in the system. Having the result of 3.18 as its total mean with a qualitative description of *Moderately Applicable*, this shows that there is a potential risk of cyber attacks in the network. There are present vulnerabilities that can be exploited which merits immediate attention such as the NIS can be remotely accessed from any location and users outside the networking staff have been granted root or administrator privileges. These intrinsic weaknesses can be harnessed by internal and external intruders to initiate attacks such as information theft, data alteration, Denial of Service Attacks (DOS), injection of malwares into the network system. The two remaining factors, a portion of the school or university deals with financial or monetary information and news stories about the school appear regularly in newspaper, magazine or website presents the university to have something of value that can be a source of curiosity or interest for cyber hackers. It may also motivate sniffers or intruders that monitor and watch the data circulating through the network to stalk or apply social engineering to acquire information for detrimental purposes.

Table 3.Security Status Assessment

Computer Security Technology	LNU	Qualitative description
Implementation of Firewalls. Firewall- A physical system or program designed to prevent unauthorized access to or from a private network.	2.71	Satisfactory
Utilization of antivirus softwares. Antivirus- A utility that looks for viruses,	2.86	Satisfactory

alerts the user and quarantines any that are found.		
Use of NIDS (Network Intrusion Detection Systems). NIDS- An intrusion detection system that examines all inbound and outbound network activity and identifies if there is somebody attempting to break or compromise the system.	2.43	Fair
Administration of System Logs. System Logs- Logs which document details of access to computer systems, such as who logged-in and which parts of the system were accessed.	2.71	Satisfactory
Use of Encryption/Decryption Softwares. Encryption-The translation of data into a format that requires a code to restore it to the original format.	2.29	Fair
Administration of E-mail logs/filters. E-mail logs/filters- Keeps tracks of incoming and outgoing messages including the sender and the recipient.	2.43	Fair
Use of Digital certificates Digital certificates- An attachment to an electronic message used for security purposes. Used to verify if the sender of a message is who he or she claims to be.	2.14	Fair
Use of reusable passwords. Reusable passwords- A simple authentication technique in which each passwords are used repeatedly for a period of time 30, 60 and 90 days, to verify an identity.	3.29	Satisfactory
TOTALMEAN	2.61	**Satisfactory**

Table 3. Present the assessment of the status and the security of information in the network systems. A total mean of 2.61 with a *Satisfactory* qualitative rating, this implies that the NIS security is weak. The results show that it needs improvement considering that it lacks in software technology to combat cyber attacks. The network security, presented in both hardware and software resources are too vulnerable for potential attack of intruders in the organization as well as the cyber space. The problem in the NIS does not lie in the expertise of the network staff but on the system requirement procured by the tertiary schools. The use of software like Intrusion Detection Systems (IDS), Encryption software, are essential considering that these software prevent undetected entries in the network traffic and confirms the authenticity, veracity, and integrity of data going in and out of the network. Email filters/logs and Digital Certificates promotes non-repudiation (Canavan, J., 2001) which restrains individuals from denying that they sent or received information, accessed a file or made a system transaction.

Table 4.Security Guidelines

Security Guidelines	LNU	Qualitative description
Protect what you consider most critical to business operations, assets and organizational functions.	4.86	Very Much Needed
Have intrusion detection so you'll know when intruders get around your defenses.	4.86	Very Much Needed
Have a security response team and a response plan.	4.71	Very Much Needed
Tighten rules for inbound traffic.	4.57	Very Much Needed
Establish a good security and disaster-recovery posture for your networks.	4.86	Very Much Needed
Control End User Access.	4.43	Very Much Needed
Restrict concurrent Log-ins for end users.	4.29	Very Much Needed
Limit the amount of disk space allocated for users.	4	Much Needed
Restrictions in location or work station	4.29	Very Much Needed
Implement time/day restrictions	3.71	Much Needed
Control access to directories and trustee rights	4.57	Very Much Needed
Restrictions of File Attributes	4.29	Very Much Needed
Restrictions of Network commands, and Executables.	4.14	Much Needed
Removal of Inactive Accounts.	3.43	Much Needed
Force anti-virus updates throughout the network and direct all users, particularly those with laptops, to power up and update their anti-virus before conducting any business on the computer.	4.57	Very Much Needed
TOTAL MEAN	4.05	**Much Needed**

Table 4.Shows the security guidelines that can be adopted to ensure a strong network infrastructure in an organization. With a total mean of 4.05 and a qualitative description of *Much needed*, this indicates the network security used by the university is inadequate and needs substantial improvement to defend against potential attacks of cyber intruders. The principle of security guidelines are meant to evaluate if the current Network Information System (NIS) of the university advocates best practices in keeping the network and its volatile resources fortified. Unfortunately, majority of the respondent choices in the security guidelines suggest there is no concrete policy or the plan for the network infrastructure does not agree with the suggested security guidelines.

VI. FINDINGS AND CONCLUSION

Based on the findings of the study, the researcher concludes that the present status of the Network information system of the Leyte Normal University deem necessary improvement. There are pressing potential risks, threats and vulnerabilities in the Network Information System (NIS) that needs adequate attention. The NIS of the institution is not secured; thus, destruction

and intrusion of vital information by viruses and hackers is inevitable.

The current Network Security policies and procedures of the university are not effective or reliable because it is not in conformity with the current network security technology. It needs to undergo system inspection and system upgrades. In addition, the solution to the problem in the network system does not lie in the expertise of the MIS alone but also on the software and hardware requirements as well. The university needs to undergo intensive evaluation and system analyses to ensure that their operation will not be hampered by malicious software or cyber hackers.

VII. RECOMMENDATION

Relative to the conclusion drawn, the researcher suggests the following recommendations:

1. The organization needs to increase the budget for Network Security and purchase the necessary network software and hardware for the protection of the system. Relevant trainings on network security by the MIS personnel and Director is strongly suggested.
2. The use of computer laboratories and other computer amenities by the administrators, instructors and students should be monitored closely to prevent unauthorized access and use of media with infected files making the NIS virus-free. This can be initiated together with the development of permissions, rights and user account guidelines and procedures.
3. Moreover, the university must strive for excellence by capitalizing on human resource thru trainings and seminars to equip the networking staff with the appropriate level of competence in their field.
4. A functional strategy for the maintenance and operation of the Network Information system (NIS) should be formulated and it must have a robust preventive, protective, response and recovery frameworks because these are the most important aspects in the network security of an organization such as a university.

REFERENCES

[1] Baker, W. H., & Wallace, L. (2007). Is information security under control: Investigating quality in information security management. *Security & Privacy, IEEE*, *5*(1), 36-44.

[2] Canavan, J. E. (2001). *Fundamentals of network security*. Artech House.

[3] Chundong, W. A. N. G., & YuKey, Z. H. A. N. G. (2014). Network Security Situation Evaluation Based on Modified DS Evidence Theory. *Wuhan University Journal of Natural Sciences*, *5*, 007.

[4] Cola, J. (2011). The Importance of Network Security And The Types Of Security Attacks. Retrieved on 10/11/2014 from http://www.jackcola.org/2011/03/the-importance-of-network-security-and-the-types-of-security-attacks

[5] Computer Security Institute (2002). CSI/FBI Computer Crime and Security Survey. Available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[6] Darmawan, N., Chong, A., Ooi, K. B., & Venggadasallam, V. A. (2009). Security Mechanism in Computer Network Environment: A Study of Adoption Status in Malaysian Company. Journal of Applied Sciences, 9(15).

[7] Farn, K. J., Lin, S. K., & Lo, C. C. (2008). A study on e-Taiwan information system security classification and implementation. Computer Standards & Interfaces, 30(1), 1-7.

[8] Gomez, M. A. (2013). AWAKEN THE CYBER DRAGON: CHINA'S CYBER STRATEGY AND ITS IMPACT ON ASEAN. In The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013) (pp. 252-261). The Society of Digital Information and Wireless Communication.

[9] Hunt, C., & Brenton, C. (2005). Active Defense—A Comprehensive Guide to Network Security.

[10] Jibao, L., Huiqiang, W., & Liang, Z. (2006, November). Study of network security situation awareness model based on simple additive weight and grey theory. In Computational Intelligence and Security, 2006 International Conference on (Vol. 2, pp. 1545-1548). IEEE.

[11] Leeson, P. T., & Coyne, C. J. (2005). Economics of Computer Hacking, The.JL Econ. & Policyy, 1, 511.

[12] Lipson, H. F. (2002). Tracking and tracing cyber-attacks: Technical challenges and global policy issues (No. CMU/SEI-2002-SR-009). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

[13] Lu, Y., & Ramamurthy, K. (2011). Understanding the link between information technology capability and organizational agility: An empirical examination. Mis Quarterly, 35(4), 931-954.

[14] Lisman, J. (2002). Administrator complacency: a real threat to network Security. SANS Institute. Retrieved from http://www.giac.org/paper/gsec /1690/ administrator-complacency-real-threat-network-security/103067 . Retrieved on January 8, 2015.

[15] Ou Yang, Yu-Ping, et al. "A VIKOR-based multiple criteria decision method for improving information security risk." International Journal of Information Technology & Decision Making 8.02 (2009): 267-287.

[16] PricewaterhouseCoopers (2000). Security Benchmarking Service/InformationWeek's

[17] 2000 Global Information Security Survey. Summary available at: http://www.pwcglobal.com/extweb/ncpressrelease.nsf/docid/7ABBA8E73B1E90 , 1D8525693500548A34.

[18] SecurityStats.com (2004). Virus Statistics, January 16, 2004. Available at: http://www.securitystats.com.

[19] Stallings, W. (2006). Cryptography and Network Security, 4/E. Pearson Education India.