International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 3 (2019) pp. 732-742

Danger of Digital Assaults in a University Computer System

Lowell A. Quisumbing

Leyte Normal University, Tacloban City, Philippines.

Abstract

The Public Universities in the Philippines are mandated by the government to deliver excellent knowledge and relevant ICT skills to students. With the emerging trends in technology, students from rural areas are migrating from the traditional use of the library books for research to using Mobile networks, Web applications, and cloud services to address information needs. Most often students focus on how to get the desired information but will lose sight of security. The study looks into the network security awareness of students in a university. The study employed a descriptive survey design where a survey instrument was given to Information Technology students of all year levels in the University to assess the level of network security in the network and the application of its concepts in their computing. The results of the study will be used as reference for future network security policies in the university.

Keywords: Network Security, Status Assessment, Security Guidelines, Hardware and Network Technology, Risk Assessment, Threat Assessment

INTRODUCTION

The utilization of the Internet and other technology advancements in the Philippine Universities has essentially expanded in the most recent decade. While its motivation and point is to advance correspondences and research in the scholarly field, it has turned into an important part of a College understudy's life.

College students employ the Internet for finding data, and gaining general learning (De Leon, J. A. V., and Tarrayo, V. N., 2014). The Internet today isn't just a data superhighway serving instructors and scholars, yet additionally another relational field in which youngsters can upgrade their chances and social encounters (Chou, C., and Peng, H., 2011). From multiple points of view, the Internet can be utilized to access email, finish coursework, buy books and arrange online exchanges that require personal data.

Be that as it may, this sort of reliance on the Internet has its traps and downsides. Utilizing the Internet routinely, opens students to various dangers, for example, introduction to unseemly or possibly unsafe data, divulgence of critical and private data, online-purchase scams, and allurement by digital predators who need to meet them face to face for impeding purposes. Subsequently, understudies who utilize the Internet are more helpless against various sorts of Cybersecurity dangers, for example, erotic entertainment, hacking, copyright encroachment, piracy, and bullying (Shields, J., & Poftak, A., 2002).

As network security threats continue to be an urgent issue, the significance of teaching and re-situating students on proper Network security practices is a vital concern. As indicated by Ng, Kankanhalli, and Xu (2009), Information security instruction including security training, security awareness, and security education programs impact students to become security conscious. Moreover, Arachchilage and Love (2014), mentioned that human factor is the most basic factor in ensuring safe web and PC usage. Guardians, educators and authorities ought to give the best possible direction and attention to students so they never stray. (Datar, T. D., Cole, K. A., & Rogers, M. K., 2014) agreed that providing a high level of security awareness should be prioritized over policies that restrict or limit the access of students to educational resources. (Vicks, M., 2013) proposes that as opposed to actualizing prohibitive approaches, it is critical to cultivate a culture of appropriate use of the network and raise information security awareness to the students instead.

Essentially, studies have demonstrated that there are shifting impacts that persuade a person's security behaviors. While technological controls are critical to the assurance of computing data, network security additionally depends on a person's perception on security (Jansen, J., 2015) More so, minimal researches have been written on the Network security practices of students and only a few have attempted to hypothetically clarify the meaning to the individual’s actions. While the behavioral comprehension of Network security practices among college understudies remains an intricate issue, it is unquestionably vital to examine the causes.

College student awareness of Information Technology (IT) security issues continues to be poor. Most college students communicate via social networking sites, oblivious of the fact that these environment is where fraudulent emails, stolen passwords, unsecured systems, and inadequate network practices are prevalent (Mensch, S., & Wilkie, L., 2011). Hence, it is but imperative that the students be made to understand the implications of engaging in these technologies. The purpose of this study is to assess the integrity of a State Universities network security through the lens of the IT students, network users who practice and use the Network Information systems. The result of the study will establish a reference for a University network security plan. The existing network information system, potential threats, network security status and security guideline are the predictors in assessing if the schools network information system is safe and effective. To evaluate the stability of a network, (Canavan, 2001; Brenton and Hunt, 2001; Stallings, 2006)

recommend that we look at the existing threats, vulnerabilities, attacks and security practices of the users that exist in the network.

This study is conceived on the idea that identifying the network security status and conditions will be beneficial to the school. It will help in the identification of vulnerabilities and weaknesses in order to formulate good and effective measures that will help the sustainability and smooth operation of the network. It is in the researcher best interest to provide more heightened security awareness on the students who use and engage in these network systems.

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 (Quisumbing, LA., 2016, 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 assets, 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 (Quisumbing, LA., 2016, 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.

RESEARCH OBJECTIVES

This study aims to determine the network security status and requirements of a State University as identified by the BSIT students. Specifically, these attempts to answer the following questions:

1. What are the demographic profiles of the BSIT students in terms of Age, Gender and Year level?
2. What is the level of proficiency of the BSIT students in terms of Computer Networking and Information Systems usage according to their own perception?
3. What is the level of awareness of the BSIT students relative to Information Security?
4. What is the extent of use of the BSIT students on the Computer Systems of the University?
5. What is the current Network Information System (NIS) status and the potential threats in the network Information Systems of the university as perceived by the BSIT students?
6. What are the current Network Security Technologies used by the University?
7. Are the current Network Security policies and procedures of the university attuned to the modern network security Guidelines?

METHODOLOGY

Design

This study utilized the Descriptive survey method. The researcher desired to know the status and other characteristics of the network security of the university as perceived by the Bachelor of Science in Information Technology (BSIT) students of the University for the period of AY. 2016-2017.

Subject

The Bachelor of Science in Information Technology (BSIT) students of the University who use the Network Information Systems for sharing and processing data to support various educational requirements are the respondents of this study. The subjects were selected from a total population of 412 BSIT students, of which 100% students were chosen. Moreover, the students came from four (4) levels starting from the freshman or first year level to the senior or fourth year level.

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 Information, Information Security Awareness, and Use of Computer Systems in the University, Existing Network Information System Assessment, Potential Threat Assessment, Security Status Assessment, and Information Security Solutions.

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 the students 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.

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 along with Google sheets and Google Forms were used to tabulate and analyse the results.

In the evaluation of Information Security Awareness of the BSIT students, the following scale was used:

Rating Scale	Qualitative Description
5	Strongly Agree
4	Agree
3	Moderately Agree
2	Disagree
1	Strongly Disagree

Below is the qualitative description of the Information Security Awareness with an interval of 0.8 to have an equal distribution of the rating scale:

Limits of Scale	Qualitative Description
4.21 – 5.0	Strongly Agree
3.41 – 4.2	Agree
2.61 – 3.4	Moderately Agree
1.81 – 2.6	Disagree
1.0 – 1.8	Strongly Disagree

In the evaluation of the BSIT Students Extent of Use of Network Computer Systems in the University, the following scale was used:

Rating Scale	Qualitative Description
5	Strongly Agree
4	Agree
3	Moderately Agree
2	Disagree
1	Strongly Disagree

Below is the qualitative description of the Extent of Use of Network Computer Systems with an interval of 0.8 to have an equal distribution of the rating scale:

Limits of Scale	Qualitative Description
4.21 – 5.0	Strongly Agree
3.41 – 4.2	Agree
2.61 – 3.4	Moderately Agree
1.81 – 2.6	Disagree
1.0 – 1.8	Strongly Disagree

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

Rating Scale	Qualitative Description
5	Strongly Agree
4	Agree
3	Moderately Agree
2	Disagree
1	Strongly Disagree

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	Strongly Agree
3.41 – 4.2	Agree
2.61 – 3.4	Moderately Agree
1.81 – 2.6	Disagree
1.0 – 1.8	Strongly Disagree

The Network Security Technology 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 Network Security Technology 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 Network Security Guidelines Assessment, 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 Network Security Guidelines Assessment 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

RESULTS AND DISCUSSION:

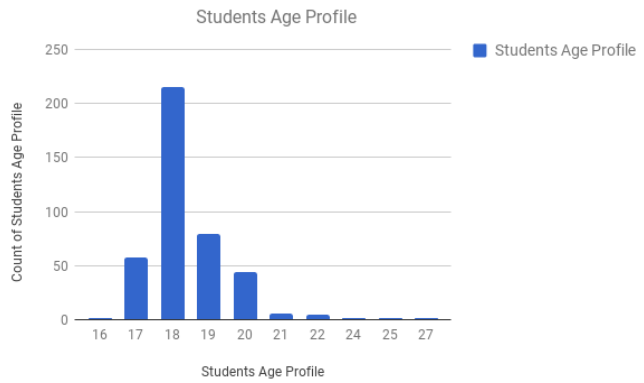

Figure 1. Age profile of BSIT students

Figure 1, Illustrates the breakdown of respondents by age. From the total number of respondents, majority (215 or 52.18%) of the respondents were 18 years of age, followed by the students aged 19 years old at (79 or 19.17%). This was followed by respondents aged 17 (57 or 13.83%), 20 (44 or 10.67%), 21 (6 or 1.45%), 22 (5 or 1.21%), and 16 (2 or 0.48%). The student age that had the lowest number of respondents were 24, 25 and 27 at (1 or 0.24%) respectively. This shows that majority of the respondents are 18 years and older. The age of the subjects was ideal for the study considering that subjects that are in their late adolescence (18-24 years of age) are considered to have developed and apply abstract thinking skills, they have greater ability to consider different points of view, increased empathy and concern for others, and new interest in societal issues for many (Newman, B. M., & Newman, P. R., 2017). This implies a positive effect on the study as the subjects that were chosen have a higher sense of understanding and relativity to the network security environment.

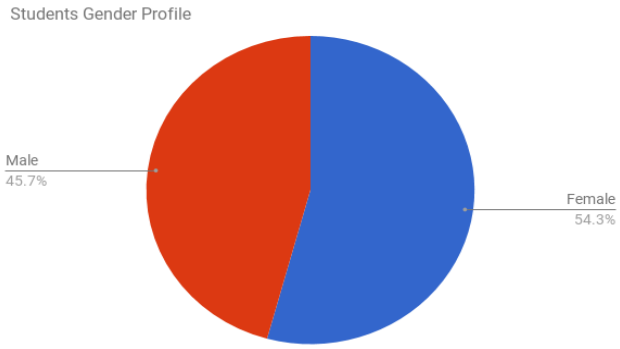

Figure 2. Gender profile of the BSIT Students

Figure 2, presents the gender profile of the respondents. Out of the total number of subjects (188 or 45.7%) were Male and (223 or 54.3%) were Female. This suggests that more female students enrolled in the BSIT program than the male students. This also proves that among those with academic degrees in the Philippines, there are more female enrollees than male enrollees (Statistics on Filipino women and men's education. (2014, May 13). Retrieved August 13, 2017, from http://www.pcw.gov.ph/statistics /201405/statistics-filipino-women-and-mens-education). This indicates a change in the enrollment trends of the past, wherein ICT and Engineering courses were commonly dominated by male students. Furthermore, it affirms that female students are more interested in pursuing careers in ICT and Communication technology today.

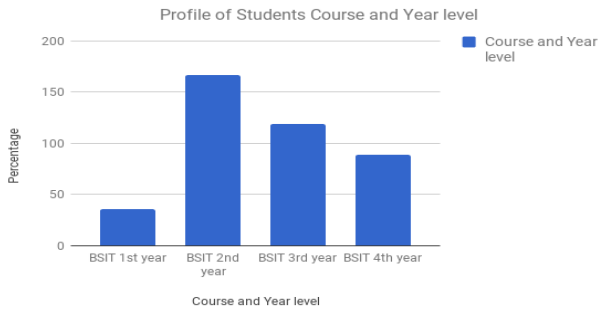

Figure 3. Course and Year Level Profile of the BSIT students

Figure 3, shows the distribution of students in terms of their course and year level. Out of the total population of 412 BSIT students, majority came from the second year level with (167 or 40.53%) respondents, the third year level with (119 or 28.88%), the fourth year level with (89 or 21.60%) students and the first year level with (36 or 9.46%) students. The demographics means there were more freshmen students or new enrollees during Academic Year (A.Y. 2015-2016) in the University compared with the succeeding years of which there was a lower percentage if not a decline in the number of new enrollees of the BSIT program. One of the significant factors that may have affected the enrollment were the number of illegible student applicants who qualified in the screening process of the BSIT program.

Figure 4, Illustrates the self-perceived proficiency of the students in Computer Networking and Information Systems usage. (259 or 64.1 %) of the students described themselves as Intermediate users, while (134 or 33.2%) considered themselves as basic users. A minimal number of students (11 or 2.7%) identified themselves as advanced users. The figure shows that majority of the respondents are knowledgeable in the area of Computer Networking and Information systems considering that both of these topics are offered as introductory subjects in the BSIT curriculum. The Routing and Switching courses from the CISCO Networking Academy Program which was integrated into the BSIT program contributed significantly into the students learning in this field. The BSIT students are perceived to be adequately prepared in answering the research instrument considering that they have a basic understanding of the topic Network Security and Information systems.

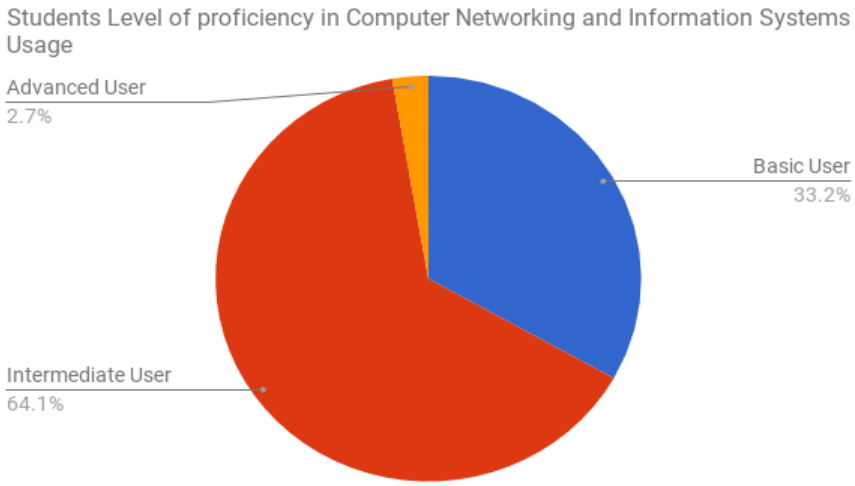

Figure 4. Proficiency in Networking

Table 1. Information Security Awareness

Information Security Awareness	**Rating**	**Qualitative description**
1. Information Security is an important part of my education.	4.74	Strongly Agree
2. I am aware that there is an existing Information Security policy and regulations in the University.	2.81	Moderately Agree
3. I have received Information Security awareness training at the University.	2.62	Moderately Agree
4. My study involved the use of research information.	4.65	Strongly Agree
5. My study involved the use of personal information	2.68	Moderately Agree
6. My study involved the use of confidential information	2.4	Disagree
7. My study involved the use of financial information	2.81	Moderately Agree
8. I am aware that there are security risks in using computers.	4.94	Strongly Agree
9. I am aware that there are threats in the university computer network.	4.44	Strongly Agree
10. I know that there are security software's that protect information.	4.75	Strongly Agree
TOTALMEAN	**3.68**	***Agree***

The table shown above (table 1) illustrate the Information Security Awareness of the BSIT students in the university with a qualitative result of ***Agree*** having a total mean of **3.68**. The findings described the level of awareness of the students towards the information that they send and receive thru the Network Information System (NIS) of the University. Majority of the items rated ***Strongly Agree*** (I am aware that there are security risks in using computers = **4.94**, I know that there are security software's that protect information = **4.75**, Information Security is an important part of my education = **4.74**) ***Moderately Agree*** (I am aware that there is an existing Information Security policy and regulations in the University = **2.81**, my study involves the use of financial information = **2.81**, my study involves the use of personal information = **2.68**). This implies that the respondents have a more than satisfactory level of awareness on the type of information that they utilize and process in the network. Furthermore, it explains that the students know what they are using and the risks that are involved in the use of technology. This is essentially important because users play an important role in the information security performance of organizations by their security awareness and cautious behavior (Albrechtsen, E., 2007). If the students are properly and adequately informed as to what to watch for, what to protect, and what to secure, this alone could prevent potential problems that could affect the infrastructure as a whole. Often, it is just awareness that is the key to prevention and protection. Awareness serves as a significant layer of security to add to existing security measures (Brodie, C., 2008). On the other hand, the lowest rated item in the table is (My study involves the use of confidential information) with a qualitative result of ***Disagree*** and a mean of **2.4**, this is significant because there are cases when users fail to identify the type of information that they put in the computer. For example, they might not realize that providing their true names, addresses and personal information on social media constitutes disclosure of confidential information, which can be the subject of identity theft and can then be used for online fraud. Students must exercise caution in providing information of any kind especially in the network of the University where hundreds of individuals are connected at any given time. They should be able to distinguish what confidential information is and what is not, to avoid security and privacy issues.

Table 2. Extent of use of Students in the Network Computers of the University

Extent of use of Students in the Network Computers of the University	**Rating**	**Qualitative description**
1. I used the computer two to three hours a day.	3.0	Moderately Agree
2. I used and exchange information with Social Media sites.	3.29	Moderately Agree
3. I searched the Network for any kind of Information.	3.18	Moderately Applicable
4. I shared my password and other log-in information with other people.	1.9	Strongly Disagree
5. I downloaded different material in the University Network.	4.5	Strongly Agree
6. I copied any kind of file to the computers in the Network.	4.67	Strongly Agree
7. I acquired data from other users in the network computers.	3.2	Moderately Agree
8. I accessed the network server remotely.	3.5	Agree
9. I visited untrusted and underground websites using the network.	3.7	Agree
TOTALMEAN	**3.43**	**Agree**

The table shown above (table 2) illustrate the Extent of use of Students in the Network Computers of the University with a qualitative result of **Agree** having a total mean of **3.43**. The findings show the degree to which the BSIT students utilize the computers in the Network of the University. Majority of the items rated ***Moderately Agree*** (I used the computer two to three hours a day=**3.0**, I used and exchange information with Social Media sites =**3.29**, I searched the Network for any kind of Information=**3.18** and I acquired data from other users in the network computers =**3.2**). The findings suggest that the student's extent of use of computers in the network have a more than average frequency involved. This implied that the frequency of using computers as well as the applications that were being utilized in the network posed a threat to its security. The students should understand that the only secure system is the system which never connects to a network and never installs software. However, with the significant importance being placed on connectivity today it is almost impossible (Darmawan, Chong, et.al., 2009). Hence, there is no way of avoiding a potential attack from both internal and external threats. Other significant findings rated ***Strongly Agree (***I downloaded different material in the University Network=**4.5** and I copied any kind of file to the computers in the Network=**4.67**). Downloading and Copying of files without restrictions or controls are considered as risky to the integrity of the Computer Network. While some of these activities may be innocuous, a potential for a security breach (Zonouoz, Houmansadr, Berthier, Borisov, & Sanders., 2013), possibly with devastating consequences, always lurks in the background because desktop computers and laptops are susceptible to multifarious forms of malicious IT infringements. Furthermore, in a study conducted by (Mylonas, 2013) users who download applications from various application repositories were found to have exhibited a blind trust in such repositories and do not necessarily exercise caution when selecting, downloading, and installing

applications. Finally, the lowest rated item in table 2, was (I shared my password and other log-in information with other people) with a qualitative result of ***Strongly Disagree*** and a mean of **1.9.** The result suggests that students know how to secure their mail and online accounts from possible intrusions. They are aware about the risk of sharing their personal accounts and are cautious on divulging critical information to other people.

Table 3. Existing Network Information System (NIS) and Threat Assessment

Existing Network Information System and Threat Assessment	**Rating**	**Qualitative description**
1. The NIS has been in full operation for more than 5 years.	4.29	Strongly Agree
2. The NIS is composed of two or more laboratories	4.57	Strongly Agree
3. There are more than fifty computers connected to the NIS.	4.57	Strongly Agree
4. The NIS is a LAN (Local Area Network).	3.4	Moderately Agree
5. The NIS is a WAN (Wide Area Network).	3.86	Agree
6. The NIS has Internet access.	3.29	Moderately Agree
7. The NIS houses vital and important assets.	3.14	Moderately Agree
8. The NIS is equipped with new and modern communications facilities such as modems, routers, switch, workstations and servers	3.14	Moderately Agree
9. The computers in the NIS are always checked and updated.	2.55	Disagree
10. The NIS is well funded in terms of maintenance and operability	3.12	Moderately Agree
11. The NIS uses new and sophisticated programs for smooth operation.	2.78	Moderately Agree
12. The NIS human resource is sufficient to its needs.	3.52	Agree
13. The NIS is being maintained by persons who are computer experts and computer literate.	4.7	Strongly Agree
TOTALMEAN	**3.61**	**Agree**

The table shown above (table 3) displays the Existing Network Information System as viewed by the University students with a qualitative result of **Agree** having a total mean of **3.61.** The results show the level of knowledge and familiarity of the students towards the network technology and its services. Majority of the items were rated ***Moderately Agree*** (The NIS is a (LAN) Local Area Network =**3.4,** The NIS has Internet access =**3.29**, The NIS houses vital and important assets =**3.14**, The NIS is equipped with new and modern communications facilities such as modems, routers, switch, workstations and servers = **3.14**, The NIS is well funded in terms of maintenance and operability =**3.12,** The NIS uses new and sophisticated programs for smooth operation =**2.78).** The results indicate that students know what valuable resources are present in the Network of the University. These assets present something costly or expensive which can be a potential target for hackers or intruders. Most cases of information theft and cyber hacking spawn from various motivation particularly in something that is considered to be valuable. Thus, by being aware of the technologies and capabilities of the network, students can anticipate and gauge the risks as well as the threat to their security. Other important factors are the items that rated ***Strongly Agree*** *(*The NIS has been in full operation for more than 5 years =**4.29**, The NIS is composed of two or more laboratories = **4.57**, There are more than fifty computers connected to the NIS =**4.57**, The NIS is being maintained by persons who are computer experts and computer literate =**4.7**) This implies that students were profoundly knowledgeable of the network systems roots, sources and the people who maintain it. It is important for the users in the network to keep a level of awareness on how data is handled, maintained and stored so that in cases where there is a breach or threat to the network system, students will find it easier to respond because they are familiar to the people and the environment. The lowest rated item in table 3 was (The computers in the NIS are always checked and updated) with a rating of **2.55** and a qualitative description of ***Disagree***. This suggests that the student's perception on the maintenance of the computers in the network was poor. Adequate attention and timely response should be given to the equipment protection and maintainability.

Table 4. Network Security Technology Assessment

Network Security Technology	**Rating**	**Qualitative description**
1. Implementation of Firewalls. Firewall- A physical system or program designed to prevent unauthorized access to or from a private network.	2.73	Satisfactory
2. Utilization of antivirus software. Antivirus- A utility that looks for viruses, alerts the user and quarantines any that are found.	2.25	Fair
3. 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.	2.41	Fair
4. 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.	2.18	Fair
5. Use of Encryption/Decryption Software. Encryption-The translation of data into a format that requires a code to restore it to the original format.	2.29	Fair
6. 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
7. 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
8. 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	**2.46**	**Fair**

Table 4. shown above presents the Network Security Technology assessment of the University network systems as perceived by the BSIT students. A total mean of **2.46** with a qualitative rating of **Fair.** The result implies that the Network Information Systems security is weak. Majority of the items rated ***Fair*** (1. Utilization of antivirus software =**2.25**, Use of Network Intrusion Detection Systems =**2.41**, Administration of System Logs =**2.18**, Use of Encryption/Decryption Software =**2.29**, Administration of E-mail logs/filters =**2.43**, Use of Digital certificates = **2.14**) The result shows that the students views on the network security status of the University needs significant improvement. The system security, defined by the technologies present in the system were powerless against potential attacks from the internal network or the internet. The utilization of Intrusion Detection Systems (IDS) and Anti-Virus Software are very important considering that these tools protect and prevent undetected passages in the system, and therefore affirms the Authenticity, veracity, and trustworthiness of information going in and out of the system. Email channels/logs and Digital Certificates promotes non-repudiation (Canavan, J., 2001) which blocks people from denying that they uploaded or downloaded data, accessed a file or made a transaction from within the system. The lowest rated items in table 4 with a qualitative description of ***Satisfactory*** were (Implementation of Firewalls =**2.73**, and Use of reusable passwords =**3.29**) These results confirm that the students understand that in using networks, it is necessary to follow certain parameter or give proper permissions to each of the employees or users of the network. Firewalls work by monitoring and managing outbound and inbound network traffic. The technology establishes a barrier between a trusted internal network and untrusted external network, such as the Internet so unauthorized network intrusions are avoided.

Table 5. Network Security Guidelines Assessment

Network Security Guidelines Assessment	**Rating**	**Qualitative description**
1. Protect what you consider most critical to business operations, assets and organizational functions.	4.86	Very Much Needed
2. Have intrusion detection so you'll know when intruders get around your defenses.	4.86	Very Much Needed
3. Have a security response team and a response plan.	4.71	Very Much Needed
4. Tighten rules for inbound traffic.	4.57	Very Much Needed
5. Establish a good security and disaster-recovery posture for your networks.	4.86	Very Much Needed
6. Control End User Access.	4.43	Very Much Needed
7. Restrict concurrent Log-ins for end users.	4.29	Very Much Needed
8. Limit the amount of disk space allocated for users.	4	Much Needed
9. Restrictions in location or work station	4.29	Very Much Needed
10. Implement time/day restrictions	3.71	Much Needed
11. Control access to directories and trustee rights	4.57	Very Much Needed
12. Restrictions of File Attributes	4.29	Very Much Needed
13. Restrictions of Network commands, and Executables.	4.14	Much Needed
14. Removal of Inactive Accounts.	3.43	Much Needed
15. 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 5. 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. Furthermore, most of the responses suggest that the majority of the Network Security Guidelines are either Needed or much Needed. This implies that University Network Infrastructure is not attuned to the current network security standards. The principle of security guidelines are meant to evaluate if the current 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 universally accepted security guidelines.

CONCLUSION

Based on the findings of the study, the researcher concludes that the present status of the Network information system of the 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 is 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.

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 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] Statistics on filipino women and men's education. (2014, May 13). Retrieved August 13, 2017, from http://www.pcw.gov.ph/statistics/201405/statistics-filipino-women-and-mens-education

[2] Newman, B. M., & Newman, P. R. (2017). Development through life: A psychosocial approach. Cengage Learning.

[3] Quisumbing, L. A. (2016). Risk of Cyber Attacks in the Network Systems of a State University in Eastern Visayas, Philippines: A Case Study.

[4] Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & security, 26(4), 276-289.

[5] Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

[6] Brodie, C. (2008). The importance of security awareness training.

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

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

[9] Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education*, *14*(1), 44-53.

[10] 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.

[11] 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

[12] Computer Security Institute (2002). CSI/FBI Computer Crime and Security Survey.

[13] Available at: http://i.cmpnet.com/gocsi/db_area /pdfs/fbi/FBI2004.pdf

[14] 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).

[15] Datar, T. D., Cole, K. A., & Rogers, M. K. (2014, January). Awareness of scam e-mails: an exploratory research study. In *Proceedings of the Conference on Digital Forensics, Security and Law* (p. 11). Association of Digital Forensics, Security and Law.

[16] De Leon, J. A. V., & Tarrayo, V. N. (2014). Cyber Reading in L2: Online Reading Strategies of Students in a Philippine Public High School. *i-Manager's Journal on English Language Teaching*, *4*(2), 8.

[17] 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.

[18] 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.

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

[20] Jansen, J. (2015). Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach. In *HAISA* (pp. 120-130).

[21] 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.

[22] Leeson, P. T., & Coyne, C. J. (2005). Economics of Computer Hacking, The.*JL Econ. & Pol'y*, *1*, 511.

[23] 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.

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

[25] 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.

[26] Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. Journal of Management Information and Decision Sciences, 14(2), 91.

[27] Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

[28] 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.

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

[30] 2000 Global Information Security Survey. Summary available at:

[31] http://www.pwcglobal.com/extweb/ncpressrelease.nsf/docid/7ABBA8E73B1E90

1D8525693500548A34.

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

[33] Shields, J., & Poftak, A. (2002). A report card on handheld computing. *TECHNOLOGY AND LEARNING-DAYTON-*, *22*(7), 24-36.

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

[35] Vicks, M. E. (2013). *An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina's K–12 Public Schools* (Doctoral dissertation, Nova Southeastern University).

[36] Zonouz, S., Houmansadr, A., Berthier, R., Borisov, N., & Sanders, W. (2013). Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. Computers & Security, 37, 215-227.