Cyber Security Awareness Among Selected Educational Institutions in Butuan City Philippines

Engr. Orlando Ritchie Natonton
ornatonton@urios.edu.ph
Engineering & Technology Program
Father Saturnino Urios University

Lorenzo Ezekiel M. Turla
lmturla@urios.edu.ph
Computer Studies Program
Father Saturnino Urios University

Nephi P. Romano, DBA
npromano@urios.edu.ph
Business Administration Program
Father Saturnino Urios University

Abstract

Internet use is becoming a daily routine for most Filipino educators and students. However, the Philippines ranked low in cultural aspect due to unintentional downloading of malwares through emails or search engines. This case study focuses on identifying and determining the level of awareness in cybersecurity of selected schools in Butuan City Philippines. This research utilizes the descriptive research model and describes the level of awareness in cybersecurity among selected and limited personnel from both government and private educational institutions in terms of experience of being breached or hacked, level of perception in security of the organization, presence of policies and procedures, presence of a unit responsible for cybersecurity awareness and monitoring, and awareness of information security attacks.

A survey questionnaire using Google Forms was used to determine the answers. The results showed that forty one percent (41%) of the responses from the private institutions have experienced virus attacks while 33% of the responses from the public educational institutions have experienced such. Fifty four percent (54%) say that their system is secure to a certain extent. While in the public experience, fifty percent (50%) mentioned that they perceived that their system is not secure.

46% of the respondents from the private institutions say that they have a dedicated department or division responsible for network security

while fifty percent (50%) of the public institutions say that they have no department dedicated for network security.

40% responses from the private educational institutions state that cyber incident response plans have been prepared by their organization. While 13% chose none of the selection or are not aware of the policies and procedures.

Fifty three percent (53%) of the responses from the private educational institution selected those presentations and discussion at conferences has raised their awareness of information security attacks while fifty percent (50%) from the public sector responded that both became aware through the conferences as well as legal and /or regulatory requirements.

There is a need for further study among educational institutions to foster preparedness especially in terms of a cyber threat or attack using other factors such as use behavior in such situations. Since almost forty one percent (41%) of the respondents have perceived that they have experienced virus infections which are probably through files downloaded which have embedded malware even though they are at PDF, DOC, and other non-detectable file extensions. The researchers recommend exploring other methods and instruments to evaluate other factors.

Keywords: Cyber security, cyber security perception, cyber knowledge, cyber awareness, cyber education, youth

1. Introduction

Internet use is becoming a daily routine for most Filipino educators and students, from social media news and email updates to school websites. The internet or the "Cloud" is important to the teachers and learners in coping with education updates and new trends. Some websites such as Google Plus, Facebook, Snapchat, LinkedIn, Twitter, Instagram, Google Gmail, Yahoo Mail, Dropbox, Google Drive, and Google sites are some of the current internet technologies used by most educational institutions in the Philippines.

Despite the massive use of the internet or cyberspace, little has been researched and investigated about the level of awareness of users in cybersecurity. Although the distinction between information and cybersecurity sometimes overlaps, the two are mostly discussed synonymously. Information security or data security focuses on confidentiality, integrity, and availability of data which is found in servers, laptops, and devices not necessarily connected to the internet. Cybersecurity, on the other hand, is protecting data in electronic form which basically is located online or in cyberspace. In some cases, authorities and school officials could only respond when a particular school's website has been maliciously hacked causing damages to certain crucial files. Most attacks such as defaced websites cause financial losses, from opportunity cost of having their website non- functional for several hours or days as well as damage to reputation of the school's ability to protect its information online. According to Kaspersky Real Time Cybermap, the top five (5) most attacked and infected countries are: Russia, Germany, Vietnam, India, and the USA, while the Philippines ranked 23rd among the most attacked countries. In the survey results in the Global Cybersecurity Index or GCI, the Philippines ranked 39th among 193 countries as of January 15, 2018. This was due to the high ratings from the legal aspect in implementing the Data Privacy Act (RA 10173), Anti-Wiretapping Law (RA 4200), the e-Commerce Law (RA 8792) and the latest Cybercrime Law (RA 10175). However,

according to study, the Philippines was low in rank in cultural aspect since most Filipinos inadvertently downloaded malwares through emails and the internet search engines. Many cases still present high rates of Filipinos responding to scam emails with attached malware in the forms of PDF or android installer file APK. Several cybercrime cases have been reported in terms of hacking, malware, cyber bullying, phishing, online scams, ransomware, and identity theft worldwide (Kaspersky, 2018).

In response to these cases, the Cyber Security Awareness campaign or CSA were researched by some countries to determine the level of citizen preparedness of a cyber threat or cyberattack. In South Africa, results of a study among students in a particular private institution revealed that twenty-four-point one percent (24.1%) have no knowledge about general secure behavior such as downloading and sharing pirated content. Eleven-point four percent (11.4%) are aware of password management, twenty seven percent (27%) are informed about cyberbullying, five percent (5%) do not know about phishing and online scams, forty- three-point one percent (43.1%) do not know about malware and or ransomware, and twenty one percent (21.7%) are responses relating to identity theft. In the United Kingdom, studies about cybersecurity awareness have been responded to since 2016. The Philippines has also responded by implementing RA 10175 (Cybercrime Law of 2012). The Philippine National Police (PNP) as well as the Department of Information and Communications Technology (DICT) has been active in their campaign to push schools to offer cybersecurity related subjects. However, despite the campaign in cybersecurity, there is a need to be updated on the level of awareness of the Filipino people in terms of being safe online most especially in the academic or educational sector. As such there is a need to evaluate the awareness of people from each region of the country. This case study focuses on identifying and determining the level of awareness in cybersecurity from selected schools in Butuan City, Philippines.

2. Related Literature

Cybersecurity awareness (CSA) is a key defense in the protection of people and systems. One of the studies for selected students has shown that instances of "cognitive dissonance" make the students (who were the subjects of their study) potentially vulnerable to cyber-attacks. Their methods involved giving a questionnaire which tested students in terms of four variables: cybersecurity knowledge, self-perception of cybersecurity skills, actual cybersecurity skills and behavior, and cybersecurity attitudes. The results suggest that there is a need for targeted CSA campaigns that could address the specific weaknesses of populations of users (Chandarman & Niekerk, 2017).

The graph below illustrates their findings:

Figure 3: Students' knowledge of six cybersecurity matters
(N = 1188, 1197, 1193, 1191, 1182, 1196)

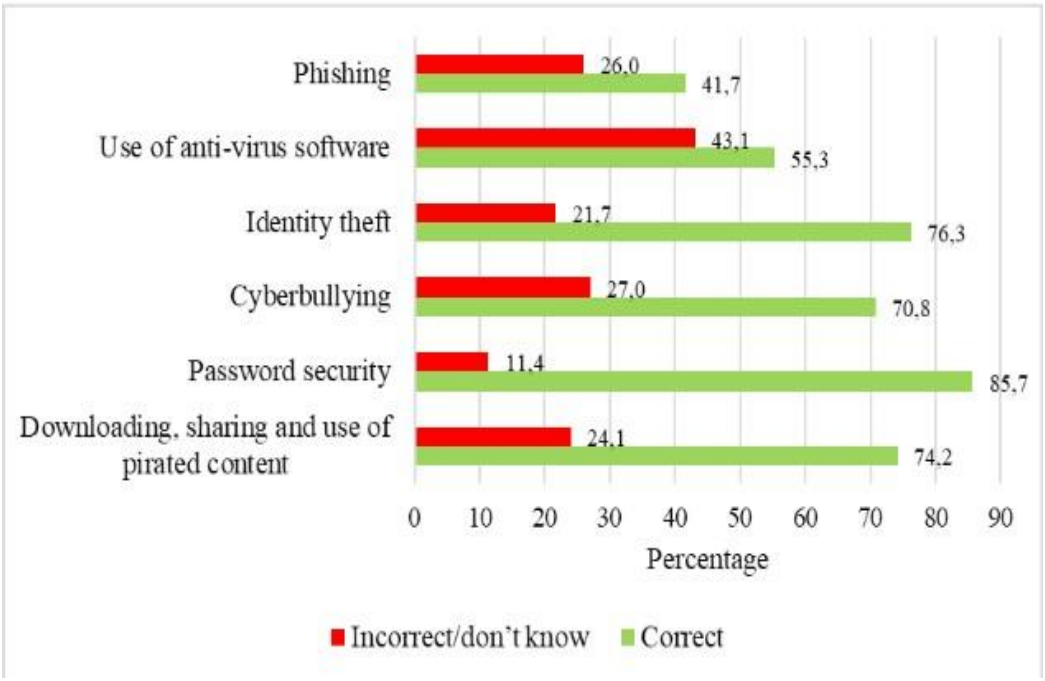

Figure 1: R. Chandarman's - Students' knowledge of six cybersecurity matters

In a study conducted by (Hadlington, 2017), he explored the relationship between risky cybersecurity behaviors, attitudes towards cybersecurity in a business environment, internet addiction, and impulsivity. The results demonstrated that internet addiction was a significant predictor for risky cybersecurity behaviors. On the other hand, a positive attitude towards cybersecurity in business was negatively related to risky cybersecurity behaviors. Interestingly, the measure of impulsivity also revealed that both attentional and motor impulsivity were significant positive predictors of risky cybersecurity behaviors, with non-planning being a significant negative predictor. The results present a further step in understanding the individual differences that may govern good cybersecurity practices. It strongly emphasizes the need for more effective training by focusing directly on the awareness mechanisms (Hadlington, 2017).

Stories of cyber-attacks are becoming a routine in which cyber attackers show new levels of intention by sophisticated attacks on networks. Unfortunately, cybercriminals have figured out profitable business models and they take advantage of online anonymity. Since most cyber incidents are human enabled, this shift requires expanding research to underexplored areas such as behavioral aspects of cybersecurity. In an effort to provide a review of relevant theories and principles, research has been conducted by (Maalem Lahcen, Caulkins, Mohapatra, & Kumar, 2020) to give insights about the matter. As a result, they proposed an interdisciplinary framework that combines behavioral cybersecurity, human factors, and modeling and simulation. Though they concluded that organizations should be involved in research to make sure that the model works the way they are intended (Rahman, Khalid, Sairi, Zizi,, & Khalid, 2020).

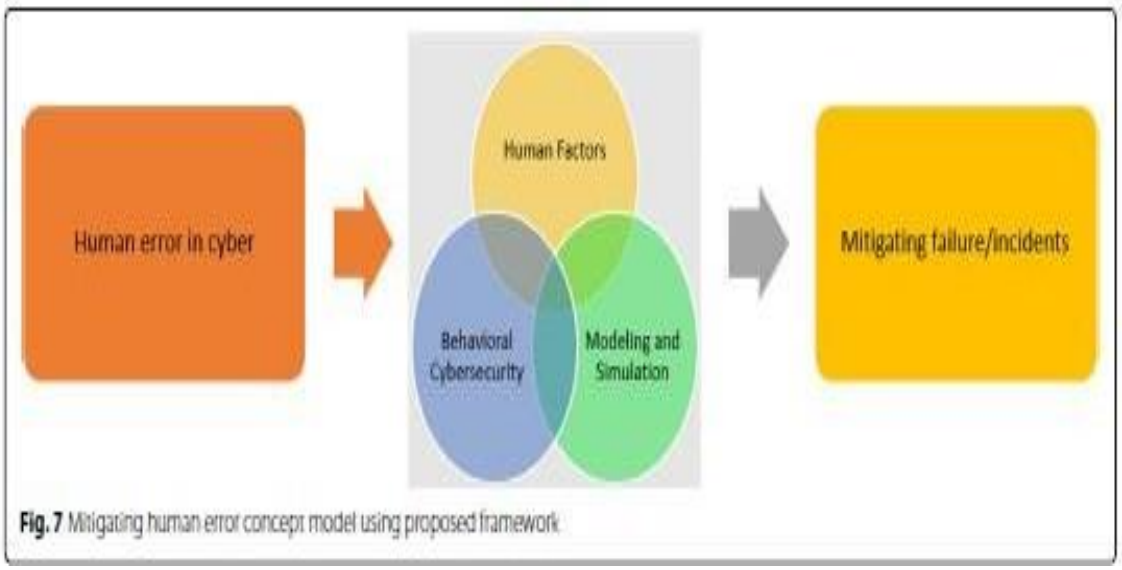

Figure 2: Lachcen's Mitigating human error concept model.

To tertiary institutions, a study was conducted by (Fatokun, Hamid, Norman, & Fatokun, 2019), which investigated if age, gender, and educational level has an impact on the cybersecurity behavior and beliefs of tertiary institution students, and to find out to what extent this difference exists. In their research, a cross-sectional survey was conducted among 340 students and Structural Equation Modelling was employed for evaluating impacts. Results show that students' cybersecurity behaviors varied based on Age for factors such as: Perceived Severity, Peer Behavior, Familiarity with Cyber Threats, Response Efficacy and Perceived Vulnerability. Gender effects also existed in Security Self Efficacy, Computer Skills, Cybersecurity Behaviors, Perceived Severity, and little effects in Prior Experiences with Computer Security Practices. Educational level differences existed in Cues to Action and Familiarity with Cyber-Threats. In summary and as a conclusion, all the three factors of age, gender, and educational level have some vital impacts on the components of cybersecurity perceptions and behaviors of students in the tertiary institution. Their findings instigate the need for specific/focused cybersecurity

training and interventions for students in the tertiary institutions (Fatokun, Hamid, Norman, & Fatokun, 2019).

In a published study of Monica Whitty, her team tried to focus particularly on the risky practice of sharing passwords. Despite the number of public advice campaigns, they hypothesize why individuals still engage in risky password practices. As they have predicted, it has been inferred that individuals who scored high on a lack of perseverance on their experiment test were more likely to share their own passwords. They also found out that age was a significant predictor of sharing passwords, as older people were more likely to share passwords (Whitty, Doodson, Creese, & Hodges, 2015).

Almost everybody has heard of cybersecurity. However, the urgency and behavior of persons do not reflect a high level of awareness. The inability to frame concepts of cybersecurity properly will result in a failure to develop appropriate policies. In a paper of (de Bruijn & Janssen, 2017), the study discussed the challenges in framing policy on cybersecurity. The limited visibility, socio-technological complexity, ambiguous impact, and the contested nature of fighting cybersecurity complicates policymaking. In their proposal, they presented evidence-based framing strategies which can help increase societal and political awareness of cybersecurity and put the issues in perspective. They argued that it is important to take the evidence as a starting point of framing the advocacy, and to avoid utopian and dystopian frames, as these typical strategies might be counterproductive (de Bruijn & Janssen, 2017).

In the Middle East, a study was conducted by (Al-Janabi & Al-Shourbaji, 2016) to understand the level of awareness of information security, the associated risks, and overall impact on the institutions. They conducted surveys to gather data and analyze the information security awareness particularly among academic staff, researchers, undergraduate students, and employees within educational environments. The results reveal

that the participants do not have the requisite knowledge and understanding of the importance of information security principles and their practical application in their day-to-day work. It was implied in the study that the situation can be corrected through comprehensive awareness and training programs (Al- Janabi & Al-Shourbaji, 2016).

Even though the internet has been advantageous to humankind, there are dangers that emerged related to the use of it. Cases like cyber-bullying, online fraud, racial abuse, pornography, and gambling had increased tremendously due to the lack of awareness and self-mechanism among internet users to protect themselves from being victims to these acts. One of the vital measures to be taken is to cultivate knowledge and awareness among internet users from an early age, i.e., young children. In a paper written by (Rahman, Khalid, Sairi, Zizi,, & Khalid, 2020), few strategies were discussed as to how cyber security education can be implemented in schools. The study tried to explore why it is so critical that modern learners are educated about the risks associated with being active in cyberspace. As a conclusion, factors such as the teacher's level of knowledge, funding, and resources are identified as the top challenges to cybersecurity in education. The general media which includes television and radio are also implied to play important roles in educating children through cybersecurity campaigns (Rahman, Khalid, Sairi, Zizi,, & Khalid, 2020).

In much recent research produced by (Wiley, McCormac, & Calic, 2020), the research attempted to explore the relationship between Information Security Awareness (ISA), organizational culture, and security culture. The results showed that while organizational culture and security culture were correlated with ISA, security culture played an important mediating relationship between organizational culture and ISA. This suggests that organizations should focus on security culture rather than organizational culture to improve ISA (Wiley, McCormac, & Calic, 2020).

In today's information-communication environment, awareness of and preparedness for digital threats is of utmost importance for organizational systems. It is not possible to fully guard against or eliminate all digital threats but with an educated awareness, management of the risks along with appropriate policies, and processes in place, organizational systems are competent to become digital resilient. In this regard, (Galinec & Luić, 2020)from Crotia proposed a model-based approach and methodology to create a model scheme, thus they created the novel Cyber Resilience Model within digital resilience.

Figure 3: Galinec and Luic's Engagement Cyber Resilience Model

Digital resilience modelling approach takes account of the components of digital threats within digital security and engagement. Further investigations are directed towards finding and enabling efficient and effective processes for agile cyber

resilience of the security information system able to cope with unforeseeable and unpredictable events in the inner and outer environment of the system (Galinec & Luić, 2020).

2.1. The Scenario

In the Global perspective, cybersecurity is a must. According to Kaspersky Real Time Cybermap, the top 5 most attacked and infected countries were: Russia, Germany, Vietnam, India, and the USA while the Philippines ranked 23rd as the most attacked country. Kaspersky's Cyberthreat Real-Time Map utilizes threats and attacks as detected from their installed software around the globe. It monitors eight areas per second namely: On Access Scan (OAS), On Demand Scan (ODS), Mail Anti-Virus (MAV), Web Anti- Virus (WAV), Intrusion Detection Scan (IDS), Vulnerability Scan (VUL), Kaspersky Anti-Spam (KAS), and Botnet Activity Detection (BAD). As of August 27, 2018, at 9:41 AM, the Philippines was ranked 24th as the most attacked country. The information in relevance to the eight areas as of the said date was: OAS (5,897 detections per second), ODS (8,578), MAV (40), WAV (8413), IDS(660), VUL (191), KAS(3118), and BAD (0). In relation to Top Infected mail using MAV in last week (August 19 to 25, 2018) the following were discovered and ranked:

1. (14.9%) Exploit. Win32. VE-2017-11882.gen.
2. (12.03%) Trojan.Win32.Crypt.gen.
3. (10.88%) Backdoor.Win32. Androm.qftz;
4. (4.98%) Dangerous Object.Multi-Generic; and
5. (4.97%) Worm.Win32.WBVB.vam. CVE-2017-11882 ranked last week and last month as No. 1 exploit detected by Kaspersky.

CVE-2017-11882 is a vulnerability that exists in Microsoft Office software. A successful attacker could take control of the affected system and then install programs; view, change, or delete

data; or create new accounts with full user rights. Such an attack could impact a great loss for educational institutions affected with such vulnerability.

In the survey results in the Global Cybersecurity Index or GCI, the Philippines ranked 39th among 193 countries as of January 15, 2018. This was due to the high ratings from the legal aspect in implementing the Data Privacy Act (RA 10173), Anti-Wiretapping Law (RA 4200), the e-Commerce Law (RA 8792), and the latest Cybercrime Law (RA 10175). However, the Philippines ranked low in cultural aspect due to reasons where most Filipinos unintentionally download malwares through emails or through search engines. Many cases still present high rates of Filipinos responding to scam emails with attached malware in the forms of PDF as well as android installer file APK. Some still enter their username and passwords in websites enabled for phishing as well as clicking links without suspecting if such link is malicious or not. Many cybercrime cases have been reported in terms of hacking, malware, cyber bullying, phishing, online scams, ransomware, and identity theft worldwide.

2.2. Global and National Cyber Security Awareness (CSA) Campaigns

In response to these cases, the Cyber Security Awareness campaign or CSA has been conducted as research by some countries to determine the level of preparedness of its citizens in case of a cyber threat or cyberattack. One of the efforts that is central to the conception of this study is the survey conducted by the Deloitte company, an Anglo-American multinational professional services network, through their Caspian region sector. Such endeavors gave insight into the information security maturity of organizations, with a focus on cyber security, and by far, one of the largest information surveys in Central Asia. The survey identified the five most relevant conclusions on the current state of information security programs in Central Asia, which were as follows: 1. Majority of companies have not been exposed to

cybersecurity incidents. 2. Information security policies, procedures and responsibilities are mostly in place and defined. 3. Insufficient controls to ensure third parties, (i.e., vendors / partners), comply with appropriate security standards. 4. Awareness of business (senior) management and end-user around cybersecurity risks is insufficient. 5. Though basic security measures are in place; more advanced solutions are uncommon. In South Africa, results of a study in the level of awareness among students in a particular private institution revealed that twenty four point one percent (24.1%) of the respondents do not have knowledge about general secure behavior such as downloading and sharing of pirated contents, eleven point one percent (11.4%) are aware of password management, twenty seven percent (27%) are informed about cyberbullying, fifty six percent (56%) do not know about phishing and online scams, forty three point one percent (43.1%) do not know about malware and or ransomware, and twenty one point seven percent (21.7%) are responses relating to Identity theft. In the United Kingdom, studies about cybersecurity awareness have been responded since 2016.

The Philippines has also responded to the cyber threats as well as attacks by implementing the Cybercrime Law of 2012 or the RA 10175. Government agencies such as the DILG-PNP as well as the Department of Information and Communications Technology (DICT) has been active in their campaign to push schools to offer cybersecurity related subjects (sunstar.com, 2017).

However, despite the campaign there is still a need to be updated on the level of awareness of the Filipino people in terms of being safe online most especially in the academic or Educational Sector.

3. Methodology

The case study utilized the descriptive research model. Describing the level of awareness in cybersecurity among selected and limited personnel from both government and private educational institutions in terms of (1). Experience of being breached or hacked, (2) Level perception in security of the organization, (3) Presence of policies and procedures, (4) Presence of a unit responsible for cybersecurity awareness and (5) Monitoring, and awareness of information security attacks. These factors are derived from the questions conceptualized in the 2014 study conducted by Deloitte in Central Asia. A survey questionnaire using Google Forms was used to determine the answers.

4. Results and Discussions

The case study focused on identifying and determining the level of awareness in cyber security from selected schools in the province of Agusan del Norte, Philippines, in terms of experience of being breached or hacked, level perception in security of the organization, presence of policies and procedures, presence of a unit responsible for cybersecurity awareness and monitoring, and awareness of information security attacks.

4.1. Profile of Respondents

a. Educational Institution Employed

i. Private Educational Institution(s) = 82.2%

ii. Government Educational Institution(s) = 11.8 %

A total of fifteen (15) respondents answered the questionnaire online. Thirteen (13) or eighty-seven percent (87%) of the respondents come from the private educational institutions

while two (2) or thirteen percent (13%) of the respondents came from government educational institutions.

1. **In terms of Experience of being breached or hacked.**

	Private Educational Institutions (n=13)	**Public Educational Institutions (n=2)**
a. Not Exposed	4	1
b. Virus	7	1
c. Hacker	2	
d. Malware	2	1
e. Stolen Assets	0	
f. Information not available	1	
g. Weaknesses highlighted during testing	1	
Total	**17**	**3**

Table 1: Have you suffered a breach or hack in the past twelve (12) months? (Multiple answers considered)

From Table 1, 7 or 41% of the responses from the respondents from the private institutions have experienced virus attacks while 33% of the responses from the public educational institutions have experienced such.

2. **Level of perception in security of the organization**

Selection	**Private**	**Public**
a. Sufficient secure	4	1
b. Secure to a certain extent	7	0
c. Info not available	2	0
d. Highly secure	0	0
e. Not secure	0	1
Total	**13**	**2**

Table 2: How secure do you think your organization's network is?

Responses from the private educational institutions reveal that seven (7) personnel or fifty four percent (54%) say that their system is secure to a certain extent. This means that fifty-four percent perceived that their system could protect them only to a certain extent. There are possibilities that the system would and could not be secure. While in the public educational institutions' experience, fifty percent (50%) mentioned that they perceived that their system is not secure.

3. Presence of policies and procedures

Selection	Private	Public
a. Cyber incident response plans	6	
b. Information security roadmap	1	
c. Business continuity plans	2	
d. Not developed but due to be developed	1	
e. Information security governance structure	1	
f. Information security strategy	2	
g. None of the Above	2	
Total	**15**	

Table 3: Which of the following (policies / procedures) has your organization documented and approved? (Multiple answers possible)?

40% responses from the private educational institutions state that cyber incident response plans have been prepared by their organization. While 13% or 2 responses chose none of the selection or are not aware of the policies & procedures.

4. Presence of a unit responsible for cybersecurity awareness

Selection	Private	Public
a. Yes, dedicated department / division	6	0
b. Yes, but as part of another department (IT or Internal Control Department)	5	1
c. No	1	1
No answer (Blank)	1	0
Total	**13**	**2**

Table 4: Does your organization have a (dedicated) department responsible for Network Security?

46% of the respondents from the private institutions say that they have a dedicated department or division responsible for Network Security while fifty percent (50%) of the public institutions say that they have no department dedicated for network security.

5. Monitoring, and awareness of information security attacks

Selection	Private	Public
a. Presentations and discussions at conferences	10	1
b. Publications in magazines, on websites and mailing lists	5	0
c. Legal and/or regulatory requirements	4	1
d. The infrastructure of our organization was under attack	0	0
e. Clients of our organization were attacked	0	0
Total	**19**	**2**

Table 5: What has raised your awareness of information on security attacks? (Multiple answers possible)

Ten (10) or fifty three percent (53%) of the responses from the private educational institution selected that presentations and discussions at conferences have raised their awareness of information security attacks while fifty percent (50%) from the

public sector responded that both became aware through the conferences as well as legal and /or regulatory requirements.

5. Summary, Conclusion, and Recommendations

	Private (n=13)	Public (n=2)
Experience of being breached or hacked	41%	33%
Level perception in security of the organization	54%	50%
Presence of policies and procedures	40%	13%
Presence of a unit responsible for cybersecurity awareness	46%	50%
Monitoring, and awareness of information security attacks	53%	50%

Table 6: Summary of Results

The case study focused on identifying and determining the level of awareness from selected schools in the province of Agusan del Norte, Philippines, in cyber security in terms of experience of being breached or hacked, level perception in security of the organization, presence of policies and procedures, presence of a unit responsible for cybersecurity awareness and monitoring, and awareness of information security attacks. Forty one percent (41%) of the responses from the respondents from the private institutions have experienced virus attacks while 33% of the responses from the public educational institutions have also experienced such. Fifty-four percent (54%) say that their system is secure to a certain extent. While in the public experience, fifty percent (50%) mentioned that they perceived that their system is not secure. 40% of the responses from the incident response plans have been prepared by their organization. 13% responses from the respondents say that procedures were done by their institution. 46% of the respondents from the private institutions say that they have a dedicated department or division responsible for network security while fifty percent (50%) of the public institutions say that

they have no department dedicated for network security. Fifty-three percent (53%) from the private educational institution responded that presentations and discussions at conferences have raised their awareness of information security attacks while fifty percent (50%) from the public sector responded that both became aware through the conferences as well as legal and /or regulatory requirements.

The need to be updated on the level of awareness of the Filipino people in terms of being safe online most especially in the academic or educational sector is a must. Since almost forty one percent (41%) of the respondents have perceived that they have experienced virus infections which are probably through files downloaded which have embedded malware even though they are at PDF, DOC, and other non-detectable file extensions.

There is a need for further study among educational institutions to foster preparedness especially in terms of a cyber threat or attack using other factors such as use behavior in such situations.

Lastly, in future studies, the researchers recommend exploring other methods and instruments to evaluate other factors.

REFERENCES

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management, 15(01), 1650007*. doi:https://doi.org/10.1142/s0219649216500076

Chandarman, R., & Niekerk, B. V. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*. doi:https://doi.org/10.23962/10539/23572

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34(1)*, 1-7. doi:https://doi.org/10.1016/j.giq.2017.02.007

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities. *Journal of Physics: Conference Series, 1339(1), 012098*. doi:https://doi.org/10.1088/1742-6596/1339/1/012098

Galinec, D., & Luić, L. (2020). Design of conceptual model for raisingawareness of Digital threats. *WSEAS TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT, 16*, 493-504. doi:https://doi.org/10.37394/232015.2020.16.50

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*. doi:https://doi.org/10.1016/j.heliyon 2017.e00346

Kaspersky. (2018). Cyberthreat Map by Kaspersky. *CyberMap*. doi:https://cybermap.kaspersky.com/

Maalem Lahcen, R., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*. doi:https://doi.org/10.1186/s42400-020-00050-w

Rahman, N., Khalid, F., Sairi, I., Z. N., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10(5)*, 378-382. doi:https://doi.org/10.18178/ijiet.2020.10.5.1393

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of

who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking, 18(1)*, 1-7. doi:https://doi.org/10.1089/cyber.2014.0179

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88, 101640*. doi:https://doi.org/10.1016/j.cose.2019.101640

WWW.URIOS.EDU.PH
Volume 16 No.2
2023