ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.3

Assessment on the Cybersecurity Awareness in Academic Institutions

May S. Hermogeno
Corporate Executive Officer II
Office of the Senior Vice President, Administrative Services Sector
Home Development Mutual Fund, Petron Mega Plaza Building, Philippines

Abstract:
Information and Communications Technology (ICT) have been a major player in our day-to-day activities and to the whole economy today. However, with the challenges brought about by the global connectivity, there is a need to fully understand what cybersecurity is, the associated risks and threats, how to mitigate the risks, best security practices, and how to properly handle security incidents. These challenges on global connectivity are not only present in the working environment but also in educational environment. The purpose of this article is to study the level of cybersecurity awareness in academic institutions. A survey research, through questionnaire, will be administered to randomly selected students, teachers, and employees of chosen academic institutions. The questionnaire will cover cybersecurity awareness (i.e., cyberbullying, password, and social media), and data privacy. The study will assess their knowledge, attitude, and behavior towards information security. Comprehensive training programs and awareness campaigns must be provided by the Administrator of academic institutions based on the result of their level of awareness.

IndexTerms: cyber threats, cyberbullying, cybersecurity, data privacy, identity theft, information security, internet, online connectivity, password, personal information, privacy, security awareness, security incident, sensitive information, social network, technology

I. INTRODUCTION

Online connectivity has been playing a vital role in everyone's lives, having it as a necessity rather than a luxury. Most of us are hooked into social media (i.e., Facebook, Instagram, YouTube, and Twitter among others), online shopping (Amazon, e-bay, Zalora, Lazada, Shopee, etc.), online games, and various mobile applications. We even used internet for checking emails, doing research works, and communicating with others. Undeniably, we can spend our whole day with our computers or mobile phones if we have online connectivity. It is the fastest way of obtaining information. Just as what everyone are saying, "Everything we need to know, we can find in the internet". However, using online connectivity entails sharing of personal information and imposes security threats. The same way those adults are into internet, the younger ones also. In previous years, there were news involving young children becoming victim of cybercrime, cyber-bullying, identity theft, and just recently, the Momo Challenge, wherein, children are given challenge to hurt others or if not, hurt themselves. Technology brings many benefits to the students in doing their homework and researches as well as to the teachers in coming up their lesson plans and delivering their lessons. It is a given fact that it is the responsibility of the parents to educate and protect their children to these kind of cyberspace incidents and threats, but since children spend more time in school, the teachers' role in inculcating safety and effective use of information technology is very crucial. The Administrators of educational institution should also be aware on how to secure information and protect the privacy of their students, teachers and staff. Given the circumstances above, the purpose of this study is to investigate what academic institutions in the Philippines can improve to increase the level of cybersecurity awareness of students, teachers, and staff. In that way, they can protect themselves from cyber-crimes, identity theft, malicious threats, and other security threats by securing their personal information and imposing best security practices, through cybersecurity education, training programs and awareness campaigns.

II. RESULTS

Information Security is simply protecting your data. According to Wikipedia, Information Security, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical. Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity. According to Secure work 2018 Incident Response Insights Report, 42% of the attackers gain entry from successful phishing scams. People are weakest link in any organization's cybersecurity defense. And that's why people are usually the first target of cyber attackers. People are easier to compromise, especially if they lack proper training in basics of security practices.

CYBERSECURITY AWARENESS

ISO/IEC 27032:2012 defined Cybersecurity as the preservation of confidentiality, integrity, and availability of information in the Cyberspace. In this digital age, securing personal information is one of the biggest challenges the Philippines is currently facing. At this point, internet security awareness become a crucial issue. On the article published by The Manila

Times on June 17, 2018, Philippines jumps to No. 12 from No. 15 regarding the highest number of Internet users worldwide, with a penetration rate of 63 percent of the population. According to the Internet World Stats, the 11 countries with highest number of Internet users are Chine, with 722 million; India, 462 million; United States, 312 million; Brazil, 149 million; Indonesia, 143 million; Japan, 118 million; Russia, 109 million; Nigeria, 98 million; Mexico, 85 million; Bangladesh, 80 million; and Germany, 79 million. However, Philippines' internet connection speed has been rated the slowest in Asia Pacific by Akamai Technologies Inc.'s State of the Internet Report. As such, Makati City Rep. Luis Campos Jr. has been urging the Congress to pass House Bill 5337, which seeks to categorize broadband or high-speed internet access as a "basic telecommunications service". Based on the statistics released in February 2019 by Statista (a Statistics Portal for Market Data, Market Research and Market Studies) for survey period of 2017 to 2018, the Philippines had 64.1 million internet users in 2017 and projected to grow to 93.7 million internet users in 2023. This includes individuals of any age who use internet from any location via any device at least once per month. A survey was also conducted for the number of mobile phone internet users of any age in the Philippines from 2017 to 2023, who accessed from mobile browser or an installed app at least once per month. The result shows that 34.5 million of people accessed the internet through their mobile phone. In 2023, the figure is projected to grow to 50.8 million mobile phone internet users. Caluza, Quisumbing, Verecio and Tibe (2018) studied the perspectives of the selected Bachelor of Science in Information Technology (BSIT) students in a Philippine State University which evaluated their habits, practices, views, issues, and experiences in cybersecurity that influences their behavioral practices in computing. The researchers have evaluated how the IT students practice cybersecurity in school, why they should need to practice cybersecurity, what experiences the IT students encountered that influenced their views, and what are the pressing issues on cybersecurity in school. It was concluded that awareness programs should be conducted to the students, teachers, and employees of the university. The researchers also recommended measures to mitigate security risks such as use strong passwords, change default passwords, develop and enforce policies on mobile devices, implement cybersecurity training program, maintain awareness of vulnerabilities, maintain an accurate inventory of control system devices, apply network firewalls, use secure remote access, and implement measures for detecting compromises, and develop a cybersecurity incident response plan. Results of the study will be used as bases for the improvements in the university BSIT program. Moreover, the study foresees promoting the development of an adaptive cybersecurity policy for the University to enforce. Omorog and Medina (2017) examined the perception of Filipinos in terms of internet security to establish the need on the part of the government to create cybersecurity culture for every Filipino. Based on their findings, there was an increase of 50% on the number of Internet Users for the last three years, wherein, 94.4% of which accessed the internet thru mobile phones. Internet users also uses free wi-fi access at malls, restaurants, and other public areas. The study disclosed that Filipinos have enough knowledge on what internet security is, but they have little understanding on the proper implementation. Thus, a need for proper education on cybersecurity awareness and training programs. Al-Janabi and Al-Shourbaji (2016) analyzed the information security awareness among academic staff, researchers, undergraduate students and employees within educational environments in the Middle East in an attempt to understand the level of awareness on information security, the associated risks and overall impact on the institutions. The results revealed that the respondents do not have the necessary knowledge and understanding of the importance of information security principles and their practical application in their day-to-day work. This situation can be corrected through comprehensive awareness and training programs as well as adopting all the mandatory safety measures at all levels of the institution to ensure that the students, academic staff, and employees are trustworthy, technology savvy and keep their data safe. The use of Internet is not only limited to one age group. Young students are more exposed to online connectivity because schools nowadays are integrating technology as a learning and communication tool. As such, these young students are more prone to security attacks due to lesser knowledge on cybersecurity. Therefore, the schools have an obligation to ensure the online safety of their students. Relative to this, the teachers must also be well-equipped with knowledge and skills, and right attitude and behavior on cybersecurity for them to be able to teach their students with self-perception and be able to protect themselves. Secondary students are chosen to be the best subject of this study because they already have advanced thinking, can decide on their own, and can already understand the situation but they are not considering the issue of security. In short, most of the times they are careless and have less experience on the effects and risks associated in using the Internet. Most of them don't think before they click. Based on the study conducted by Pramod and Raman (2014), they have found out that secondary students are aware of the security concerns regarding online connectivity but at the same time, are not fully aware of all the security risks and necessary security best practices. According to Tekerek and Tekerek (2013), the 2,449 elementary and high school students they have investigated have sufficient level of information and computer security awareness in terms of ethical issues but low level of awareness in terms of knowledge about the rules. Some of the risks students are facing are easy access to illegal sites, sites with violence and sex contents, communication with unreliable people, child abuse and over dependence on games. With the modern technology and advanced mind of the kids today, educational institutions should equip the students with the right knowledge and skills about information security awareness so as to control the negative effects of using the internet. Alhejaili (2013) stated that Internet bring many benefits to students, and somehow an integral part of the success of students in schools. Internet can provide students the answers and information about anything. In the contrary, using the internet as a source of education also provides many risks as well as negative effects on the behavior of the students if not properly used. The researcher believed that teaching security awareness for secondary school students through a web interactive program is crucial for reducing the risks that might have an effect on the students. Moreover, the result of the study of Al-Jerbie and Jali (2014) to the 10 Libyan secondary school students (aged between 13-18 years old) shows that the students have insignificant level of security awareness but still lack of proper practice of the information security. Therefore, conducting cybersecurity training program is important to avoid the security risks. The three issues discussed in this study are: cyber-bullying, social networks, and passwords.

Cyber-bullying. It is the use of technology such as Internet, mobile phones or other devices to harass, threaten or embarrass other people. The incidents of cyberbullying in the present era are increasing, wherein, young individuals were involved and commonly happened at schools. Cyber-bullying can be through personal act, picture or video clipping, text message, phone call, email, instant messaging, via websites and social media such as the very popular Facebook and Twitter. Cyber-bullying knows no age, gender, size, or social standing. It is an act of violence that can have a severe impact on the child's proper development and leaving the victims with terror and trauma, along with the possibility of committing suicide. Umesh, Ali, Farzana, Bindal and Aminath (2018) investigated the context of cyber-bullying from the viewpoints of students and teachers, and the measures to undertake to reduce cyber-bullying. A total of 230 students and 72 teachers participated in the study, wherein 61% of the students have experienced being cyber-bullied, and the most prevalent form of cyber-bullying was spreading rumors over social media. Furthermore, Niguidula, Vargas, Caballero, Marquez, and Hernandez (2017) studied the opinion of students in the Philippines regarding cyber-bullying which can be attributed to the social media. They concluded that existence of policies and procedures related to cyber-bullying can help the students, parents, teachers, and the entire school administration understand the implications of cyber-bullying to students' behavior and performance. These activities can increase the awareness on cyberbullying, that it is a crime, and it affects the social behavior of the students in school or outside of school.

Social Networks. In the present day, Cybersecurity is still a big concern. People all over the world, young and old, are hooked on social media. Undeniably, it's been part of our daily routine, that without it, our day is not complete. The main concern though is how to protect the social media users and the social media platform from cybercrime. Social Media has been using for cyber-bullying and identify theft. Khan and Haque (2017) defined social media as online communications that allows individuals to create and share information via virtual communities and networks. The popular examples of social media are Facebook, Instagram, Twitter, and LinkedIn. Facebook and Instagram are social networking sites that allows users to upload pictures and videos, send messages, share photos, and many more other features. Twitter is a micro blogging social network site that allows users to broadcast small posts called tweets. While LinkedIn is designed for professional interaction worldwide especially for business community. In 2023, the number of social network users in the Philippines is estimated to be around 62.5 million, up from 51.5 million in 2017. While the number of Facebook users within the Philippines is predicted to reach 49.9 million in 2023, up from 41.2 million in 2017 (www.statista.com, 2019). UNICEF, in its annual flagship report, The State of the World's Children 2017: Children in a digital world, presented the impact of the internet and social media on children's safety and well-being. The increase in children's vulnerability to risks and threats was also observed. In addition, the Report also identified the various positive developments to protect children online and the practical recommendations to have more effective policy and employ the best security practices. Students, teachers, and all social media users should be well-informed of the social media policy and security for them to be aware on what information to share or not. To protect oneself while using social media, one must be aware of the cybersecurity techniques to solve cyber-crime related problems as well as social ethics and social responsibility. Children must be taught of digital literacy to keep them informed and safe online.

Passwords. It is a character string used to authenticate an identity. It is a protection for ones' access to personal information. It must be regarded as a confidential information and must not be disclosed to any other person. Whitty, Doodson, Creese and Hodges (2015) found that individuals were still engaged in risky practices of sharing password despite of various public awareness campaigns. Result of their findings were considered for cybersecurity educational campaigns. Every internet users whether using it for personal or official use and whatever devices being used should know how to manage their password, i.e. use strong passwords, change password regularly, do not share password, and have different passwords for different account. In relation to the studies done for cybersecurity awareness of students, it is also important that teachers are also educated in terms of security awareness and good practices. However, it is worthy to note that being aware does not mean being hundred percent protected. According to Caparino (2018), the responsibility of educating the youth regarding cyber security falls mostly on educators. The administrators of education institutions should develop cybersecurity programs for educators. To quote what UNICEF Executive Director Anthony Lake said: "In a digital world, our dual challenge is how to mitigate the harms while maximizing the benefits of the internet for every child. The internet was designed for adults, but it is increasingly used by children and young people – and digital technology increasingly affects their lives and futures. So digital policies, practices, and products should better reflect children's needs, children's perspectives, and children's voices."

DATA PRIVACY

Advancement in technology makes our daily lives easier and somehow cheaper, but most of us are not privy that our personal information is getting compromised. This personal information can be stolen when we make an online purchase, use social media, and check emails among others. This also applies to students who spend more time doing school activities online especially in this new era, wherein, information technology plays an important role in education. In this digital era, Privacy must be a priority. There are many ways that the risk of stolen information be reduced or eliminated, and it starts with cybersecurity awareness. Cybersecurity and data privacy are interrelated. Data privacy simply means protecting your personal information, including the sensitive one. Data is an asset, that's why we should keep it safe. With the pursuit of the Philippines Government to protect every Filipinos in digital world, Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA 2012) was created to protect individual's personal information in Information and Communications Systems in Government and Private Sector, creating for this purpose the National Privacy

Commission (NPC). Correspondingly, implementing rules and regulations were promulgated to effectively implement the provisions of the Act. DPA 2012 defines Personal Information as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. While sensitive personal information refers to individual's race, ethnic origin, marital status, age, color, affiliations (religious, philosophical, political), health, education, genetic or sexual life, any proceeding for any offense committed or alleged to have been committed by the individual, Government-issued personal numbers such as SSS, GSIS, PhilHealth, Pag-IBIG and LTO, and previous or current health records and tax returns. The popular data privacy breaches reported in the Philippines includes the following:

a. Comeleak Data – the massive leak of voters' data handled by COMELEC. It was the worst recorded breach on a government-held personal database in the world, based on sheer volume.
b. Uber data breach – personal data of estimated 171,000 Filipino citizens consisting of drivers and passengers were exposed.
c. Data breach on Wendy's PH website – it was estimated that 82,150 records were exposed, which included personal details such as names, contact numbers, home addresses, hashed passwords, transaction details, and mode of payment of the customers, loyalty card members, and even job applicants.
d. Vulnerabilities on the online ordering system of Jollibee – the data of 18 million people in the online delivery database of popular fast food chain were in high risk of being exposed to harm due to vulnerabilities in the system though database has not been breached.
e. Facebook data breach – 1.2 million Filipinos were affected by this data breach, wherein information may have been improperly shared with Cambridge Analytica.
f. BPI Data Breach – an internal process involving the production data of the current and savings account database of BPI caused a massive data breach that affected the majority of its users using its online account management facility.
g. Multiple government website breach – there were schools, institutions and local government units who sustained data breaches following an organized attack on government and commercial organizations. These includes Taguig City University, Department of Education offices in Bacoor City and Calamba City, Province of Bulacan, Philippine Carabao Center, Republic Central Colleges in Angeles City, and Laguna State Polytechnic University, among others.
h. Public School Teacher in debt due to identity theft – the victim received notifications from three banks saying that he borrowed a total of Php800,000.00 in salary loans, but denied applying for the said loans. However, the victim remembered posting a photo of his Professional Regulation Commission (PRC) ID, which may be the source of information of the intruders.

Development and implementation of Privacy Management Program is the starting point to comply with the Data Privacy Act of 2012. It will lead organizations toward a culture protective of data privacy rights of individuals as part of their corporate governance responsibilities. Foregoing considered, every individual using information technology must know their rights and how to protect their personal information, must be aware of the risks involved in sharing information, and must be knowledgeable on how to handle data breaches. Benjamin Franklin once aforesaid, "An ounce of prevention is worth a pound of Cure".

III. SUMMARY

Pramod, et.al. (2014) and Al-Jerbie, et.al. (2014) found out that students have insignificant level of security awareness but still not fully aware of the security risks and proper practices of the information security. Caluza, et.al. (2018), Omoro, et.al. (2017), and Tekerek (2013) concluded that educational institutions should equip students, teachers, and staff with proper education on cybersecurity awareness and training programs. With the rapidly changing environment, where cyber attackers are everywhere, a wide range of education, training, and seminars should be conducted for the benefit of everyone. It is important that one is informed of the simple steps to take to protect oneself, their families, work place, and devices.

IV. REFERENCES

[1]. Statista. Number of Internet users in the Philippines from 2017 to 2023 (in millions), 2019. Retrieved from https:// www. statista.com/statistics/221179/ internet-users-philippines/

[2]. Number of mobile phone internet users in the Philippines from 2017 to 2023 (in millions), 2019. Retrieved from https://www.statista.com/statistics/558756/number-of-mobile-internet-user-in-the-philippines/

[3]. Number of social network users in the Philippines from 2017 to 2023 (in millions), 2019. Retrieved from https:// www. statista.com/statistics/489180/number-of-social-network-users-in-philippines/

[4]. Number of social network users in the Philippines from 2017 to 2023 (in millions), 2019. Retrieved from https:/ /www. statista.com/statistics/490455/number-of-philippines-facebook-users/

[5]. The Manila Times. PH jumps to No. 12 in highest number of Internet users, 2018. Retrieved from https:// www. manila imes.net/ph-jumps-to-no-12-in-highest-number-of-internet-users / 409083/

[6]. Securework 2018 Incident Response Insights Report. Cybersecurity Awareness Training: Network Protection and Cybersecurity Threat Best Practices, 2018. Retrieved from www.securenetworks.com

[7]. UNICEF. The State of the World's Children 2017: Children in a digital world, 2018. Retrieved from https:// www. Unicef .org/publications/index_101992.html.

[8]. Omorog, C.D. and Medina, R.P. Internet Security Awareness of Filipinos: A Survey paper. International Journal

of Computing Sciences Research, 2017; 1(4), 14-26. Doi:10.25147/ijcsr.2017.001.1.18. Retrieved from https:// www. researchgate.net/ publication/325036716 _Internet_ Security_ Awareness_of_Filipinos_A_Survey_Paper

[9]. Al-Janabi and Al-Shourbaji. A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management, 2016; Volume 15, No. 1, 1650007 (30 pages). Retrieved from https://www.researchgate.net/publication/292672963_A_Study_of_Cyber_Security_Awareness_in_Educational_Environment_in_the_Middle_East

[10]. Al-Jerbie, S.I and Jali, M.Z. A Second Look at the Information Security Awareness among Secondary School Students. Proceedings of the International Conference on Information Security and Cyber Forensics, Kuala Terengganu, Malaysia, 2014; 88. Retrieved from https:// www .academia .edu/8648765/A_SecondLook_at_the_Information_Security_Awar eness_among _Secondary_School_Students

[11]. Pramod, D. and Raman, R. A Study on the User Perception and Awareness of Smartphone Security. International Journal of Applied Engineering Research, 9(23), 19133-19144, 2014.

[12]. Tekerek, M. and A. Tekerek. A Research on Students' Information Security Awareness. Turkish Journal of Education, 2013; Vol. 2 Issue 3. Retrieved from https:// www. Research gate. net/ publication/310743923_A_Research_on_ Students'_ Information_ Security_ Awareness

[13] Alhejaili, H. Usefulness of Teaching Security Awareness for Middle School Students. Thesis. Rochester Institute of Tech nology. 2013. Retrieved from https:// scholarworks. rit. edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=6541&context=theses

[14]. Umesh B, Ali NN, Farzana R, Bindal P, Aminath NN. Student and Teachers Perspective on Cyber-Bullying. Journal of Forensic Psychology, 2018; 3: 132. doi:10.4172/2475-319 X. 10 00132. Retrieved from https://www.longdom.org/open-access/student-and-teachers-perspctive-on-cyberbullying-2475-319X-1000132.pdf

[15]. Niguidula, J.D., Vargas, E., Caballero, J.M., Marquez, P.s., and Hernandez, A.A. Senior High School Students Cyber bully ing Experience: A Case of University in the Philippines. Conference paper, 2017. Retrieved from https:// www.researchgate.net/profile/Alexander_Hernandez4/publication/324692240_Senior_High_School_Students_Cyberbullying_Experience_A_Case_of_University_in_the_Philippines/links/5add8296a6fdcc29358b791f/Senior-High-School-Students-Cyber bullying-Experience-A-Case-of-University-in-the-Philippines.pdf?origin= publi c cation_detail

[16]. Maximo, S.I. and Loy, N.S.N.G. Bullying Among High School Students as Influenced by Parent-Child Attachment and Parenting Styles. Philippine Journal of Psychology, 2014; 47(2), 125-152. Retrieved from https://www.pap.org.ph/ sites/default/files/upload/pjp2014-47-2-pp125-152-maximoloy-bullying_am on g_high_school_students_ as_influenced _by_ parent-child _attachment_and_parenting_styles.pdf

[17]. Khan, M. and Haque, S. Cyber Security and Ethics on Social Media. Journal of Modern Development in Applied Engineering & Technology Research, 2017; Vol. 1, Issue 2, 51-58. Retrieved from https://www.academia.edu/35029133/CYBER_ SECURITY_ AND_ETHICS_ON_SOCIAL_MEDIA

[18]. Whitty, M., Doodson, J., Creese, S. and Hodges, D. Individual Differences in Cyber Security Behaviors: An Examination of Who is Sharing Passwords. Cyberpsychol Behav Soc Netw, 2015; 18(1): 3-7. Retrieved from https://www .ncbi.nlm. nih.gov/pmc/articles/PMC4291202/

[19]. Caparino, E.T. Teacher's Perception on Cyber Security. Advance Science Letters, 2018; Volume 24, Number 11, 8471-8475(5). Retrieved from https://www .ingentaconnect .com/ content/asp/ asl /2018 /0000 0024 /00 000 011 /art00148

[20]. Caluza L.J. B., Quisumbing, L.A., Verecio R.L., and Tibe, D.S. Views on Cybersecurity Principles and Practices: The case of BS Information Technology Students of LNU, Tacloban City, Philippines. International Journal of Social Science and Economic Research, 2018; Volume 3, Issue 01. Retrieved from https://www .researchgate.net/ publication/326504458_ VIEWS_ ON_CYBERSECURITY_PRINCIPLES_AND_ PRACTICES_THE_CASE_OF_BS_INFORMATION_TECHNOLOGY_STUDENTS_OF_LNU_TACLOBAN_CITY_PHILIPPINES