Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Towards A Safe Cyberspace In Higher Education: Assessment Of The Cybersecurity Practices In A State University In The Philippines

DELIA THERESA C. ESCOBAR

Faculty, College of Information and Computing Sciences, Cagayan State University, Philippines.

Abstract

Generally, this study investigated the cybersecurity practices of the faculty members, students, and administrative staff of Cagayan State University, Philippines. The researcher utilized mixed method research design to describe the cybersecurity practices of the respondents. Eight campuses of Cagayan State University were used as locale of the study and there were 1,555 respondents. The study revealed that the respondents' level of cybersecurity practices is highly favorable, and this was consistent along the five dimensions namely: Malware, Password Usage, Online Scam Phishing and Social Engineering. Furthermore, the administrative staff have more favorable cybersecurity practice compared to students and faculty members. Through the findings of the study, a policy framework on cybersecurity is being proposed. The framework focuses on technical, administrative, and procedural measures that will protect critical infrastructure and increase resilience of ICT and ICT-enabled environments within the university. The framework has the following core functions: Protect, Detect, Respond, and Recover which is adopted from the National Institute of Standards and Technology Cybersecurity.

Keywords: Cybersecurity, Practices, Cyberspace, Higher Education, Cybersecurity Policy Framework

Introduction

Cybersecurity is an essential concern for nearly all organizations nowadays (Moller, 2020). As a result of the epidemic, practically all transactions and activities in higher education are now conducted online, therefore guaranteeing cybersecurity has become the gold standard for all colleges. Providing a safe and secure cyberspace for students, teachers, staff, and administrators is the current trend in managing higher education institutions, despite the fact that the country is in a transition period from distant learning to face-to-face sessions. University transactions and activities have been shaped by digital technology, which will continue to be vital and indispensable in the future (Nozaleda et.al, 2021).

Moreover, cyberattacks and data breaches are on the rise. Students and university workers are frequently the institution's weakest security links. This is the situation since it is obvious that academic members and administrative personnel occasionally disregard the significance of a password's security. In contrast, students click on dangerous URLs and attachments and utilize prohibited software programs. Even school administrators are uninformed of vital data management practices, such as encryption, and frequently disregard them. These actions by students, staff, and administrators all have the potential to result in data loss. Consequently, updated cybersecurity rules can assist all university members in understanding how to preserve the security of data and applications.

Given that information systems are essential to the University's teaching, research, and administrative responsibilities, it is of the utmost importance that all University members contribute to assuring the availability, integrity, confidentiality, and validity of the data they retain or access (Putra et.al, 2020). In addition to having the potential to undermine the institution's reputation and operations, mishandling university property puts the organization at risk of legal action. Moreover, the loss or unintended disclosure of personal information can create a significant deal of pain for the affected individuals. Therefore, it is essential to undertake a study on the cybersecurity practices of the university's academic community.

Despite the widespread use of cyberspace in academic settings, little research has been conducted on the cybersecurity practices of internet users, with an emphasis on academic community members. While cyber security awareness is an essential topic to address, it is especially crucial to examine the actions of students, teachers, and administrators in higher education. This is due to the fact that phishing assaults are increasingly targeting students, faculty, and administrative personnel. In addition, because the majority of teachers and students are enrolled in online programs and courses, the amount of time spent online increases the vulnerability of college and university data and personal information. Due to their exposure to online education, they are a prime target for hackers. Students and a few staff members were victims of cybercrime, as evidenced by their Facebook posts and personal accounts. Some claim that unauthorized access was gained to their accounts, while others assert that their passwords were compromised. Still others assert that their bank accounts were fraudulently accessed as a result of phishing.

In light of these circumstances, the researcher investigated the academic community's cybersecurity practices at Cagayan State University to provide a cybersecurity policy framework that could serve as an example for State Universities and Colleges in the region.

Methodology

Research Design

This study used Mixed Method Research Design. It used descriptive and causal-comparative research design to describe the cybersecurity practices of the respondents and determine if there is a significant difference on their practices. On the other hand, sequential explanatory research design was used to validate the results of the quantitative analysis. This is particularly focused on the explanations and elaborations of the study participants relative to the quantitative data. Sequential explanatory design consists of two distinct phases: quantitative followed by qualitative (Creswell et al. 2003). In this design, the quantitative data is collected and analyzed first. Then the qualitative (text) data are collected and analyzed second to help explain, or elaborate on, the quantitative results obtained in the first phase. The second, qualitative, phase builds on the first, quantitative, phase, and the two phases are connected in the intermediate stage in the study.

Locale and Respondents of the Study

This study was conducted in the eight campuses of Cagayan State University (CSU). The CSU or Pamantasang Pampamahalaan ng Cagayan is the largest state institution of higher learning in the Cagayan Valley Region, in terms of enrollment and number of curricular program offerings. The respondents were composed of students, faculty members, and administrative staff. The faculty members considered in this study were those holding ETL not more than 9 units. The sample size was computed using the Slovin's formula and stratified random sampling was employed. The margin of error in this study was set at 0.05. There were 1157 students, 217 faculty members, and 181 Administrative staff who participated in the study.

Research Instrument

There are two instruments used in this study. The first instrument is the cybersecurity practices questionnaire. It is composed of 50 items and respondents indicate how often they practice each statement using a 4-point Likert scale. Also, these items in the five dimensions of cyber-attacks - phishing, password usage, social engineering, online scamming and malware. Each dimension consists of 10 items. The tool is adapted from the study of Muniandy et.al (2017) on cybersecurity behavior of students in higher education in Malaysia. The Cronbach alpha for its dimensions are: malware (0.841), social engineering (0.859), online Scam (0.707), phishing (0.703), and password usage (0.702). The instrument also has undertaken content and face validity prior to its use in the study.

Lastly, the second instrument was an interview guide which elicited the explanations to the quantitative result of the study. The instrument also has undertaken content and face validity prior to its use in the study.

Data Analysis

Means, median, frequencies, percentages were used to describe the data. As the variables did not meet the requirement of normality, nonparametric techniques were used in hypothesis testing. Specifically, the Kruskal-Wallis H with Dunn-Bonferroni post hoc test was used to determine significant differences among the groups of respondents in the level of practice on cybersecurity attacks. All analyses were tested at 0.05 level using IBM SPSS. For the in-depth interview, the study participants were interviewed through video call. Two study participants were simultaneously interviewed narrating their explanations regarding the results of the quantitative data. Others opted to just send the interview guide and forward their answers to the researcher. Interviews were transcribed and thematically analyzed.

Results and Discussion

Level of Cybersecurity Practices of the Respondents

Table 1 presents that the cybersecurity practices of the respondents are highly favorable (x=3.40). Such finding means that the respondents have appropriate intention, belief or desired action in the use of internet that secures their online activities. This finding may be attributed to the fact that they are more cautious in securing their online activities because of the increasing number of victims of cybersecurity problems. A student shared a neighbors' experience on loan scams: We have a neighbor who took out a loan online and then when he couldn't pay, everyone texted in the phonebook when the neighbor said about the debt. Our neighbor had a trauma due to that experience. [S4]. This is a similar experience shared by an administrative staff: I did not know that the loan application extracted all the contact details from my phone remotely. Though I didn't get a loan, it's scary that someone out there, you don't know, can access your personal files. Immediately, I uninstalled the application [A2]. Notably, the finding is consistent with the statement of Castelo Gomez et.al (2020) who argued that with the increased use of technology for teaching, learning and continuing school operations in today's remote environment, schools have also become more vulnerable to cyberattacks. In relation to the findings of the present study, the highly favorable practice of the respondents is contrary to the study of Omorog & Medina (2020) that students do not have adequate knowledge and comprehension of the internet risks in their practical and day-to-day application.

Among the dimensions of cybersecurity practices, the respondents have highly favorable practice on malware (x=3.43) which signifies that they perform acts that would not expose their computers from viruses, worms, trojan horses and spyware. They believe that these malicious programs can steal, encrypt or delete sensitive data, alter or hijack their data. The increasing awareness of the academic community on malware is attributed to the proliferation of computing devices in almost all households. A faculty member has this to say: Even before the pandemic, I was already aware of computer viruses. I am a frequent victim, in fact, of missing and lost files. I even paid a professional just to recover my files [T1]. This finding is an affirmation of the findings of Pandey et.al (2020) who mentioned that since computers, whether handheld or desktop, have become staple in all industries, people have mastered to a certain degree common issues and problems in their devices and viruses and malwares are one of the most common problems for computers.

On the other hand, the respondents have highly favorable practice on social engineering (x=3.41) which indicates that they know how to counter manipulation techniques of hackers especially in gaining private information, access, or valuables. It also means that they are capable of determining "human hacking" scams that lures them in exposing their data, and giving access to restricted systems. For example, a student shared her experience on identity theft, I thought I know pretty well how to navigate Facebook, but I was wrong. One friend of mine sent me a message about a poser account. It was not mine, but that account uses my pictures. I reported the account and fortunately Facebook acted on it. That experience made me more knowledgeable about securing safe spaces online [S2]. This finding is explained by the fact that there are already warning appear and free online application that help the respondents secure their data. The highly favorable practice of the respondents against social engineering can be attributed to their increased level of awareness of the mechanisms of social engineering. This claim is supported by Aldawood et.al (2020) whose team revealed that the awareness of social engineering is a positive predictor of security-protective practices. The authors mentioned that due to the warning prompts that many websites have nowadays, internet users are now becoming careful of clicking malicious links.

Meanwhile, the highly favorable practice of the respondents on Online Scam issues (x=3.41) illustrates that they are smart in determining fraudulent scheme of dishonest individual, group, or company in an attempt to obtain money or something else of value. A narrative of a teacher supports this finding when she said: I am frequently bombarded with emails from research publication houses or organizations I did not even subscribe. When I check on author fees, it’s too high and unreasonable. There I saw that some of these publishing houses are fraudulent. To avoid these, I marked those emails as spam [T7].

Interestingly, their highly favorable practice in Phishing (x=3.39) signifies that they are able to determine an attack masquerade that distributes malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims. As one administrative staff said: When I download applications in my smart phone, I read the user agreement first. I am careful on what I approve accessible for the application [A1].

Finally, their highly favorable practice in Password usage (x=3.38) means that they are capable of keeping and managing their password for many purposes such as logging into accounts, retrieving e-mail, accessing applications, databases, networks, and web sites. One student narrated: I use alphanumeric characters for my password. I do not use my ID number because sometimes my classmates know my ID number [S8]. Additionally, a faculty shared these words: For my password, I refrain from using personal information already. In the past, I used my birthdate because that would be convenient for me. I realized it’s not safe because of so many safety issues nowadays [T6]. This practice is also supported by one administrative staff who said: I use unpredictable phrases or words for my password. I also vary them for multiple accounts. It's hard to be complacent with just one password. When one knows about it, then all your accounts will be affected[A5]. The highly favorable practice may be accounted to the fact that the respondents are directly or indirectly learning from news or advertisement on fraudulent means of scammers (Datta et.al, 2020).

Table 1. Cybersecurity Practices of the Respondents

	Students	**Faculty Member**	**Administrative Staff**	**TOTAL**

Cybersecurity Practices	**Mean**	**Mean**	**Mean**	**Mean**
Malware issues	3.20 (Favorable)	3.49 (Highly Favorable)	3.59 (Highly Favorable)	3.43 (Highly Favorable)
Password usage issues	3.20 (Favorable)	3.44 (Highly Favorable)	3.51 (Highly Favorable)	3.38 (Highly Favorable)
Phishing	3.23 (Favorable)	3.44 (Highly Favorable)	3.50 (Highly Favorable)	3.39 (Highly Favorable)
Social engineering issues	3.19 (Favorable)	3.48 (Highly Favorable)	3.55 (Highly Favorable)	3.41 (Highly Favorable)
Online scam issues	3.17 (Favorable)	3.47 (Highly Favorable)	3.56 (Highly Favorable)	3.40 (Highly Favorable)
Overall practices	**3.20** (Favorable)	**3.47** (Highly Favorable)	**3.54** (Highly Favorable)	**3.40** (Highly Favorable)

Legend:

1.0 -1.74	=	Highly Unfavorable
1.75-2.49	=	Unfavorable
2.50-3.24	=	Favorable
3.25-4.00	=	High Favorable

Differences on the Level of Cybersecurity Practices Among the Respondents

Table 2 shows the comparison on the level of cybersecurity practices among the respondents. The result showed that there was statistically significant difference in the level of practice in malware issues ($H_{(2)} = 115.275$, $p < 0.001$), password usage issues ($H_{(2)} = 74.893$, $p < 0.001$), phishing ($H_{(2)} = 74.248$, $p < 0.001$), social engineering issues ($H_{(2)} = 122.120$, $p < 0.001$), online scam issues ($H_{(2)} = 123.462$, $p < 0.001$) and as a whole on cybersecurity practices ($H_{(2)} = 122.009$, $p < 0.001$) among the different groups of respondents. Specifically, the administrative staff have a significantly favorable level of cybersecurity practice, or a more favorable practice compared to students and faculty members. However, the level of cybersecurity practice of students and faculty members are not significantly different. This finding maybe accounted to the nature of their work. In fact, a response from one administrative staff can confirm this finding. He said: Of course, especially in the HR office, there are so many sensitive information of employees that need to be protected. Unlike teachers, we in the administrative handle's diverse types of information across all stakeholders, from students, teachers, and from everybody in the university [A2]. Zwilling et.al (2022) argued that as custodian of records, administrative staff tend to be more protective of the data in their offices. Their inability to secure their records will have significant effect on their performance and efficiency. Also, the finding of Evans et.al (2016) is affirmed because teachers and students of computing practices are low and there was no significant difference observed. This also coincides with the study of Las Johansen et.al, (2018) which revealed that teachers and students lack awareness on cybersecurity issues and security measure and have poor cybersecurity practices. This is evident from the answer of a faculty member who said that: There are so many things to still learn especially in cybersecurity. I think, cybersecurity is more than having antivirus installed in my computer. For now, I can't fully realize the essence of cybersecurity [T2].

Table 2. Comparison on the Level of the Cybersecurity Practices Among the Respondents

		Percentile			Mean Rank
		25th	Median	75th	
Malware issues					
	Students	2.80	3.30	3.80	708.42^{A}
	Faculty Member	3.10	3.80	4.00	962.42 ^{A}
	Administrative Staff	3.10	3.90	4.00	1012.93 ^{B}
Password usage issues					
	Students	2.89	3.22	3.67	722.12 ^{A}
	Faculty Member	3.00	3.67	4.00	928.37 ^{A}
	Administrative Staff	3.11	3.67	4.00	966.50 ^{B}
Phishing					
	Students	2.90	3.20	3.80	722.91 ^{A}
	Faculty Member	3.00	3.70	4.00	917.27 ^{A}
	Administrative Staff	3.00	3.90	4.00	974.87 ^{B}
Social engineering issues					
	Students	2.90	3.20	3.70	706.48 ^{A}
	Faculty Member	3.00	3.90	4.00	964.38 ^{A}
	Administrative Staff	3.30	3.90	4.00	1022.96 ^{B}
Online scam issues					
	Students	2.90	3.40	3.70	706.34 ^{A}
	Faculty Member	3.00	3.80	4.00	960.24 ^{A}
	Administrative Staff	3.35	4.00	4.00	1028.89 ^{B}
Overall practices					
	Students	2.91	3.26	3.63	706.16 ^{A}
	Faculty Member	3.00	3.71	4.00	963.94 ^{A}
	Administrative Staff	3.14	3.79	4.00	1025.55 ^{B}

Mean ranks of the same letter are not significantly different at .05 level

The CSU Cybersecurity Policy Framework

The CSU Cybersecurity Policy Framework combines the results of a research on the knowledge and practices in cybersecurity of the CSU community and the Key Strategic Initiatives stated in the National Cybersecurity Plan 2022 of the Department of Information and Communications Technology. The proposal is also congruent to the Vision and Mission of the university in becoming a globally recognized university in technological fields while being safe, responsive and productive service provider to the community (Nozaleda, 2019). The framework has the following core functions: Protect, Detect, Respond, and Recover which is adopted from the National Institute of Standards and Technology Cybersecurity

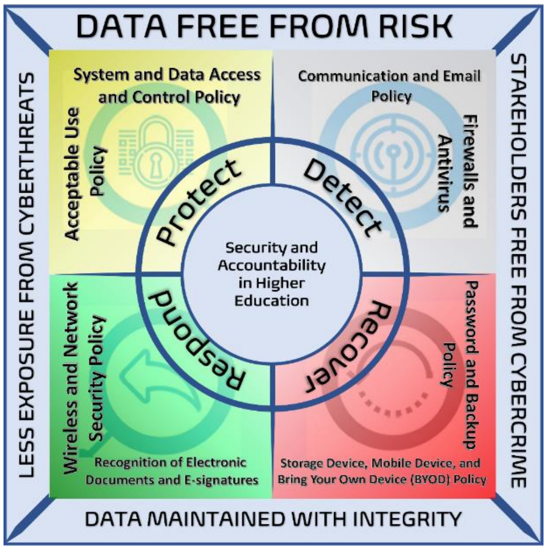
DATA FREE FROM RISK
LESS EXPOSURE FROM CYBERTHREATS
STAKEHOLDERS FREE FROM CYBERCRIME
DATA MAINTAINED WITH INTEGRITY
System and Data Access and Control Policy
Acceptable Use Policy
Communication and Email Policy
Firewalls and Antivirus
Wireless and Network Security Policy
Recognition of Electronic Documents and E-signatures
Password and Backup Policy
Storage Device, Mobile Device, and Bring Your Own Device (BYOD) Policy
Protect
Detect
Respond
Recover
Security and Accountability in Higher Education

Figure 1. Proposed Cybersecurity Policy Framework

The framework resembles a dartboard. It shows that the ultimate target is security and accountability in higher education. The framework itself is intended to be as broad as possible by categorizing and covering all cybersecurity capabilities, processes, and operations. It does this by focusing on the core functions of cybersecurity. Under each function, the specific group of policies identified in the research on knowledge and practices of the CSU community were aligned. In essence, cybersecurity relates to the confidentiality, integrity, and availability of computer systems, network systems, information systems, and other areas related to the protection of information assets. Therefore, the framework focuses on technical, administrative, and procedural measures that will protect critical infrastructure and increase resilience of ICT and ICT-enabled environments within the university. Below shows the policies that are aligned to each core function. However, it must be noted that the activities under the core functions can be conducted concurrently and continuously. Hence, the policies are technically overlapping relative to the four core functions.

Table 3. Core Functions and Policies of the Proposed Cybersecurity Policy

Core Functions	Policies
Protect This function concerns the implementation of appropriate information security safeguards that align with the environments and information classification levels. Examples of common safeguards include multifactor authentication and endpoint encryption.	○ **System and Data Access and Control Policy** ○ **Acceptable Use Policy**
Detect The university must deploy the means to proactively detect potential threats, as conventional protective measures are not enough in an era of increasingly sophisticated attacks.	○ **Communication and Email Policy** ○ **Firewall and Antivirus**
Respond When a potential security incident is detected, it is vital that the university has a documented set of procedures for dealing with it. This function concerns the key roles and actions that must be taken in such an event.	○ **Wireless and Network Security Policy** ○ **Recognition of Electronic Documents and E-signatures**
Recover Security incidents often result in unscheduled downtime. As such, this function deals with the mitigation strategies needed to restore affected capabilities and services with minimal damage to the university.	○ **Password and Backup Policy** ○ **Storage Device, Mobile Device, and Bring your Own Device (BYOD) Policy**

Ultimately, the framework shows the expected results of this set of cybersecurity policies. It is hoped that from the effective execution of these policies, the university shall have data free from risk and maintained with integrity and all internal and external stakeholders shall enjoy an academic environment free from cyberthreats and crimes.

Conclusion and Recommendations

The level of cybersecurity practices of the academic community in Cagayan State University is highly favorable and this is consistent along the five dimensions namely: Malware, Password Usage, Online Scam Phishing and Social Engineering. Notably, among the three groups of respondents, the administrative staff have more favorable cybersecurity practice compared to students and faculty members. Hence, much is desired to capacitate the students and faculty members through the proposed cybersecurity policy. Lastly, a similar study needs to be conducted but with the inclusion of officials of the State Universities and Colleges (SUC's) to comprehensively examine the concept of cybersecurity knowledge and cybersecurity practices of Higher Education Institutions (HEIs).

References

Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does awareness of social engineering make employees more secure?. International Journal of Computer Applications, 177(38), 45-49.

Castelo Gómez, J. M., Carrillo Mondéjar, J., Roldán Gómez, J., & Martínez Martínez, J. L. (2021). A context-centered methodology for IoT forensic investigations. International Journal of Information Security, 20(5), 647-673.

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced mixed methods research designs. Handbook of mixed methods in social and behavioral research, 209(240), 209-240.

Datta, P., Tanwar, S., Panda, S. N., & Rana, A. (2020, June). Security and Issues of M-Banking: A Technical Report. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1115-1118). IEEE.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9(17), 4667-4679.

Las Johansen, B. C., Quisumbing, L. A., Verecio, R. L., & Tibe, D. S. VIEWS ON CYBERSECURITY PRINCIPLES AND PRACTICES: THE CASE OF BS INFORMATION TECHNOLOGY STUDENTS OF LNU, TACLOBAN CITY, PHILIPPINES.

Möller, D. P. (2020). Introduction to Cybersecurity. Cybersecurity in Digital Transformation, 11-27.

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. J. Inf. Assur. Cyber Secur, 2017, 1-13.

Nozaleda, B. M. (2019). Awareness, acceptance, and understanding of Cagayan State University stakeholders towards its vision, mission, goals, and objectives. International Journal of Advanced Research in Management and Social Sciences, 8(6), 313-326.

Nozaleda, B. M., Dayag-Tungpalan, M., Arao, H. F., Ramos, C. C., & Mabborang, M. H. (2021). Linking College Learners' Competence in Information and Communication Technology and Learning Styles during the COVID-19 Pandemic. Turkish Journal of Computer and Mathematics Education, 3256-3262.

Omorog, C. D., & Medina, R. P. (2020). Internet Security Awareness of Filipinos: A Survey Paper. arXiv preprint arXiv:2012.03669.

Omorog, C. D., Gerardo, B. D., & Medina, R. P. (2018, September). The performance of blum-blum-shub elliptic curve Pseudorandom Number Generator as WiFi protected access 2 security key generator. In Proceedings of the 2nd International Conference on Business and Information Management (pp. 23-28).

Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International journal of information management, 55, 102171.

Putra, A. P., Akrim, A., & Dalle, J. (2020). Integration of high-tech communication practices in teaching of biology in indonesian higher education institutions.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. Journal of Computer Information Systems, 62(1), 82-97.