Journal of Positive School Psychology
2022, Vol. 6, No. 5, 4839–4850

http://journalppw.com

Cybersecurity Knowledge of The Cagayan State University Academic Community: Basis for Cybersecurity Policy

Delia Theresa C. Escobar, PhD
College of Information and Computing Sciences
Cagayan State University – Carig Campus, Philippines

Abstract

Generally, this study investigated the cybersecurity knowledge of the faculty members, students and administrative staff of Cagayan State University. The researcher utilized descriptive-correlational design to answer the research questions. Eight campuses of Cagayan State University were used as locale of the study and there were 1,555 respondents. The results revealed that the top two online activities of the respondents are messaging applications like Facebook messenger and videoconferencing like Zoom, Google Meet and MS Teams. The least online activity is downloading and uploading videos. Notably, the respondents' level of cybersecurity practices is highly favorable. The test of difference showed that students have a significantly lower level of exposure in downloading and using software application than faculty members and administrative staff. Furthermore, the administrative staff has the highest cybersecurity knowledge while the students have the lowest. The study concludes that the members of the academic community of Cagayan State University (CSU) are well informed about the aspects, importance and effects of cybersecurity. Such awareness is translated into positive cybersecurity practices which may have reduced their exposure to cybercrimes. Among members of the CSU academic community, the students need more improvement on cybersecurity knowledge and cybersecurity practice as compared to the faculty members and administrative staff. Hence, much is desired to capacitate them through the proposed cybersecurity policy.

Keywords: Cybersecurity, Knowledge, Higher Education, Cybersecurity Policy

Introduction

The pandemic has forced educational institutions to utilize internet technologies in delivering instruction. The internet has become a pervasive channel between teachers and learners' virtual communications. With its vast platforms like social media, storage clouds, learning management systems, and real-time audiovisual messaging tools, the internet paved way for a wide and infinite virtual area for learning. However, the internet is not a secured space. It is an area where there are not so many regulations. Though the Philippines has passed the Cybercrime Prevention Act of 2012 (Heffron, 2014), otherwise known as Republic Act No. 10175, critics say that the law has loopholes and is prone for ambiguous interpretations.

A demonstration of how the internet can become unsafe is a "zoombombing" incident in a private grade school in the country. A synchronous class being conducted via Zoom video conferencing was hacked, exposing the students to lewd pictures posted by an uninvited participant. This shows that some popular video conferencing applications, particularly Zoom, are susceptible to hacking (Schneider, 2021). This revelation raises serious concerns for teachers, students, school administrators, and other stakeholders as schools continue their online classes, many of which are conducted via video conferencing. In this sense, the threats of unregulated freedom of information technology may outweigh the advantages of its uses in education.

This report points to how pervasive cyber threats have become and that cybersecurity has to be reinforced. Contrary to the popular belief that hackers target only big companies, attacks have been increasingly common to home and small office, like in schools' routers, as well. This is because hackers hunt poorly managed computer systems (Pan, Zhong, & Mei, 2015) with varied intentions frequently for monetary gain. In certain cases, administrators and school officials were only able to react when the website of a specific school was maliciously compromised, causing harm to some critical files. Many attacks, such as defaced websites, cause financial losses from the opportunity cost of making their website non-functional for several hours or days and harm to the credibility of the school's ability to defend its data online (Geers, 2011).

In terms of the status of cybersecurity in the country, the Philippines was ranked 23rd as the most affected country in the world way below Vietnam, India, and the United States of America (Kaspersky, 2018). In fact, it is ranked 39th out of 193 countries in terms of Global Cybersecurity Index or GCI. This was attributed to the high legal scores for the enforcement of the Data Privacy Act (RA No.10173), the Anti-Wiretapping Act (RA No. 4200), the e-Commerce Act (RA No. 8792) and the new Cybercrime Act (RA No. 10175). Despite this impressive global standing, since most Filipinos unknowingly download malware from emails or via search engines, the Filipinos are in high risks to becoming victims of cyber bullying due to their lack of awareness and cultural inclination to simply download everything in the net. (Gonzales, 2014).

In relation with the current situation in education, many applications needed for online learning are not free to download and use. Productivity tools like word processors and presentation software require a subscription fee from the users. This forces many students and even teachers to download pirated or cracked applications and software to meet their educational needs. For many reasons, they have become relaxed in denying access to downloaded mobile applications of their personal information and data. While tools may have reached them for free, they nonetheless pose multiple threats to their privacy and personal information largely in terms of hacking, malware, cyber bullying, phishing, online scams, ransomware, and identity theft. The need for cybersecurity awareness campaigns is thus undisputed, as these remain the first line of defense in providing employees, students, teachers, and other stakeholders with the know-how of interacting safely online.

Little has been studied on the extent of knowledge of internet users, focusing on the members of academic community in spite of the heavy usage of cyberspace in such setting. While knowledge of cyber security is an essential concern to address, it is rather particularly important that focus has to be given to students, faculty members and administrative staff in higher education. This is because students, faculty members and administrative staff are becoming a priority for phishing attacks. Moreover, with the amount of time spent online, data from colleges and universities and personal information of teachers and learners is at greater risk because most are enrolled in online programs and courses. As they are exposed to online instructional modality, they are a great target for hackers. Facebook post and narratives of the students and some faculty members of CSU reveal that at a certain extent, they were victims of cybercrime. Some claim that their accounts were illegally accessed while some say that their passwords were hacked. Still others claim that they were victims of phishing because their bank accounts were fraudulently accessed. In view of these context, the researcher sought to uncover the cybersecurity knowledge of the Cagayan State University Academic Community. This is with the end in view of proposing a cybersecurity policy for Cagayan State University which maybe a model for State Universities and Colleges in the region.

Methodology

Research Design

This study used descriptive-correlational research design. The descriptive-correlational examined the respondents' online activities, cybersecurity knowledge, and the cybersecurity practice. It also tested the relationships between the variables. Descriptive correlational studies describe the variables and the relationships that occur naturally between them (Quantitativa, 2007).

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 elicits the online activities and frequently downloaded and used software applications of the respondents. The respondents chose their online activities by ticking the box that correspond to their online activities and the frequency of use of the software applications was measured using a 5-point Likert scale.

Meanwhile, the second instrument measured the cybersecurity knowledge of the respondents on the cybersecurity policies which are relevant to the activities in Higher Education Institutions. It is composed of 61 items distributed along the seven dimensions of cybersecurity policy: system and data access and control; communication and email; acceptable use, password/passphrase; backup; wireless policy, network security, and website; and, storage device, mobile device, bring your own device policy. Each item was answered using a 4-point Likert scale. The questionnaire was subject to content and face validation before it was officially used in the study. The computed Cronbach Alpha is 0.811.

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 exposure in downloading and using of software applications, level of knowledge on cybersecurity policy, and level of practice on cybersecurity attacks. Kendall's tau-b correlation was run to determine the relationship between cybersecurity knowledge and cybersecurity practice. All analyses were tested at 0.05 level using IBM SPSS. Partial least squares path modeling analysis was used to determine the relationship of awareness level of cybersecurity policy to the level of practice in cybersecurity attacks. After which, multi-group partial least squares analysis was then run to compare the differences between groups of respondents. All analyses were tested at 0.05 level using IBM SPSS and SmartPLS.

Results and Discussion

Online Activities of the Respondents

The Table 1 shows the online activities done by the respondents. Majority of the students (92.5%), faculty members (86.3%) and administrative staff (87.3%) use messaging app like Facebook Messenger with a total percentage of 91.0%. Such is followed by joining meetings in videoconferencing tools like Zoom, Google Meet ang MS Teams (85.2%). This finding implies that the said applications are essential online tools of the respondents in their undertakings. Faculty members, students and administrative staff in the new normal make use of messaging apps like Messenger to communicate in their transactions. Because face to face meetings is not allowed, they have become accustomed with the use of videoconferencing tools like Zoom, Google Meet and MS Teams. As such, the use of video sharing tools have become apparent among students (Nozaleda et.al, 2021) and teachers during the COVID19 pandemic. The finding supports the study of Akçayır (2017), on the use of social media like Messenger and Facebook in education. Accordingly, these social media applications help the students, faculty members and parents to get more useful information, to connect with learning groups and other educational systems that make education convenient.

Meanwhile, downloading and uploading videos is the least online activity of the respondents with a total percentage of 47.9%. This may be accounted to the fact that some students are reliant on the use of data only and video downloading and uploading entail additional cost on their part. With respect to the faculty members, the finding may suggest that they don't have much video learning resource to upload because making personal instructional videos are difficult to make.

Table 1. Online Activities of the Respondents

	Students		**Faculty**		**Administrative Staff**		**Overall**	
	Freq	Percent	Freq	Percent	Freq	Percent	Freq	Percent
Social Networking Activities like Facebook and Twitter	770	66.4	146	66.7	142	78.5	1058	67.9
Using messaging apps like Facebook Messenger in communicating	1072	92.5	189	86.3	158	87.3	1419	91.0
Downloading and Uploading videos in YouTube and other video hosting sites	530	45.7	121	55.3	96	53.0	747	47.9
Accessing Email Services	799	68.9	177	80.8	152	84.0	1128	72.4
Using search engines in browsing Information from the internet	830	71.6	128	58.4	100	55.2	1058	67.9
Watching movies related to the lesson	834	72.0	95	43.4	70	38.7	999	64.1
Accessing Learning Management System like the CSU-LENS	924	79.7	126	57.5	82	45.3	1132	72.6
Uploading and downloading reading materials and modules	926	79.9	138	63.0	83	45.9	1147	73.6
Editing documents, photos, and videos online	773	66.7	71	32.4	77	42.5	921	59.1
Joining meetings in videoconferencing tools like Zoom, Google Meet ang MS Teams	1003	86.5	180	82.2	146	80.7	1329	85.2
Downloading applications to be used in your studies like Microsoft office or Adobe Applications	825	71.2	85	38.8	60	33.1	970	62.2
Converting file formats online like from pdf to word	848	73.2	100	45.7	90	49.7	1038	66.6

None	7	0.6	3	1.4	0	0.0	10	0.6

Level of Exposure of the Respondents in Downloading and Using Software Applications

Table 2 shows that the level of exposure of the respondents in downloading and using of software applications is *high* (x=3.66). This finding implies that the faculty members, students and administrative staff have extensive experience in downloading and using different software applications. In today's set-up, different classes, conferences, seminars and forums are using various software applications. Among the different software applications, the three groups of respondents have *very high* exposure to word processing software (x=4.47), presentation software (x=4.25), video-teleconferencing software (x=4.41) and social networking (x=4.41). This finding connotes that Word Processing Software, Video-teleconferencing software and social networking are the most utilized platforms to carry out the respondents' classes and meetings as there was an incredible increase in the use of these platforms in this pandemic time. This supports the study of Jacobs-Israel & Moorefield-Lang (2013) that the increased use of video as a teaching medium is encroaching into traditional face-to-face teaching in higher education. This affects lecturers, students, Universities and Colleges and there is a need to bridge the gap in digital competencies.

On the other hand, the software to which the respondents have moderate level of exposure are Database software, Information Worker Software, Simulation software and Software for Engineering and Product Development. This finding means that they rarely download and use these applications. Such maybe accounted to the fact that these software applications are complex and used only in major or specialized subjects.

Table 2. Level of Exposure of the Respondents in Downloading and Using Software Applications

Software Applications	**Students**	**Faculty Member**	**Administrative Staff**	**TOTAL**
	Mean	Mean	Mean	
Word processing software	4.14 (High)	4.68 (Very High)	4.60 (Very High)	4.47 (Very High)
Database software	2.65 (Moderate)	2.85 (Moderate)	3.09 (Moderate)	2.86 (Moderate)
Spreadsheet software	2.80 (Moderate)	4.25 (Very High)	4.19 (High)	3.75 (High)
Multimedia software	3.14 (Moderate)	3.74 (High)	3.66 (High)	3.51 (High)
Presentation Software	3.88 (High)	4.52 (Very High)	4.35 (Very High)	4.25 (Very High)
Information Worker Software	3.19 (Moderate)	3.00 (Moderate)	3.12 (Moderate)	3.10 (Moderate)
Educational Software	3.18 (Moderate)	3.69 (High)	3.61 (High)	3.49 (High)
Simulation Software	2.49 (Low)	2.66 (Moderate)	2.77 (Moderate)	2.64 (Moderate)
Content Access Software	3.94 (High)	3.85 (High)	3.82 (High)	3.87 (High)
Social Networking	4.16 (High)	4.58 (Very High)	4.48 (Very High)	4.41 (Very High)
Application Suites	3.78	4.31	4.23	4.11

	(High)	(Very High)	(Very High)	(High)
Video-Teleconferencing	4.33 (Very High)	4.48 (Very High)	4.41 (Very High)	4.41 (Very High)
Software for Engineering and Product Development	2.41 (Low)	2.86 (Moderate)	2.97 (Moderate)	2.75 (Moderate)
OVERALL	3.39 (Moderate)	3.80 (High)	3.79 (High)	3.66 (High)

Legend:

1.0 -1.79	=	Very Low
1.8 -2.59	=	Low
2.60-3.39	=	Moderate
3.40-4.19	=	High
4.20-5.00	=	Very High

Level of Cybersecurity Knowledge of the Respondents

Table 3 illustrates that the level of cybersecurity knowledge of the respondents is very high (x=3.47). Such finding denotes that the respondents are very knowledgeable about the different aspects, activities, importance and effects of cybersecurity. This includes (a) System and Data Access and Control Policy; (b) Communications and Email Policy; (c) Acceptable Use Policy; (d) Password/Passphrase Policy; (e) Backup Policy; (f) Wireless Policy, Network Security and Website Policy and Storage Device, Mobile Device, Bring Your Own Device Policy. The very high knowledge of the respondents maybe explained by the fact that they are very much exposed to the experiences of people who are victims of cybersecurity problems as exposed in televisions, newspapers, radios and social media.

Among the items of cybersecurity knowledge, the respondents have very high knowledge along Wireless Policy, Network Security, and Website Policy (x=3.54) which implies that they are aware in preserving the veracity and safety of their gadgets and they practice the security measure in protecting their information. For instance, they are very knowledgeable in accessing secured sites to visit and safe wireless network to browse. Certainly, they were already able to experience using safe sites or may have learned safe sites from friends and other forms of media. The finding confirms the study of Husak et.al (2021) when they found a similar result on the knowledge level of certain members in business enterprises, the impressive awareness of the community of network security policy is due to the immersion of the business world to the cyberspace. The longer the exposure of people to the cyberspace, they become aware on how to safely navigate the environment. The same can be inferred with the CSU academic community since all facets of the activities in the university, in one way or another, are conducted online.

On the other hand, the policy which obtained the lowest mean but still with very high knowledge is Storage Device, Mobile Device, Bring Your Own Device Policy (BYOD) (x=3.39). Such finding reveals that the respondents are aware that each external and portable storage device must be under the responsibility of a specific person who shall always track its whereabouts and functionality. It also means that in the event of loss, the responsible Staff and Faculty must immediately inform their Privacy Focal Person in order to commence the remote wiping process through the CSU Management Information System Office. However, it cannot be discounted that this policy received the lowest rating among all policies. The aforementioned responses are supported by several studies arguing that in many workplaces, employees often neglect the policies set for BYOD like personal mobile devices. For instance, Palanisamy (2022) revealed very low compliance on BYOD policies because the employees feel that their devices are personal to them and whatever rules set for their work don’t apply to their private life, which includes the way they use their personal devices. The findings of this study corroborate that of Aliyu et. al, (2020) revealed that there is a satisfactory level of computer security and ethics awareness among teachers. Additionally, Senthilkumar & Easwaramoorthy (2017) observed the same positive results in which they concluded that most of the teachers have high knowledge on the basic concepts of cybersecurity and on the best practices of protecting their devices from malware, viruses, and scams.

Table 3. Level of Cybersecurity Knowledge of the Respondents

	Students	**Faculty Member**	**Administrative Staff**	**TOTAL**
Policies	Mean	Mean	Mean	
System and Data Access and Control Policy	3.35 (Very High)	3.40 (Very High)	3.56 (Very High)	3.44 (Very High)
Communications and Email Policy	3.41 (Very High)	3.39 (Very High)	3.55 (Very High)	3.45 (Very High)
Acceptable Use Policy	3.36 (Very High)	3.52 (Very High)	3.61 (Very High)	3.50 (Very High)
Password/Passphrase Policy	3.43 (Very High)	3.51 (Very High)	3.65 (Very High)	3.53 (Very High)
Backup Policy	3.47 (Very High)	3.42 (Very High)	3.51 (Very High)	3.47 (Very High)
Wireless Policy, Network Security, and Website Policy	3.48 (Very High)	3.48 (Very High)	3.66 (Very High)	3.54 (Very High)
Storage Device, Mobile Device, Bring Your Own Device Policy	3.34 (Very High)	3.34 (Very High)	3.48 (Very High)	3.39 (Very High)
Overall Policy	**3.41** (Very High)	**3.44** (Very High)	**3.57** (Very High)	**3.47** (Very High)

Legend:

1.0 -1.74	=	Very Low Knowledge
1.75-2.49	=	Low Knowledge
2.50-3.24	=	High Knowledge
3.25-4.00	=	Very High Knowledge

Difference in the Level of Exposure in Downloading and Using Software Applications among Respondents

Table 4 shows the comparison on the level of exposure in downloading and using software applications among the respondents. The result showed that there was a statistically significant difference in the level of exposure in downloading and using of software applications among the different groups of respondents, $H_{(2)} = 82.848$, $p < 0.001$. Specifically, students have a significantly lower level of exposure in downloading and using of software applications compared to the faculty members and administrative staff. Meanwhile, the level of exposure in downloading and using of software applications between faculty and administrative staff are not significantly different. This result is rather unexpected because students are supposed to be more exposed to downloading and using software applications than their counterparts. This study is contrary with the finding of Arrosagaray & González-Peiteado (2019) who revealed that the students have significantly higher frequency in downloading applications than their teachers. However, the lower exposure of the students in downloading and using software applications may be attributed to their capacity to use various applications. Unlike teachers and the administrative staff, students do not have the same level of financial capacity to buy their devices. This finding affirms the finding of de los Santos (2020) who revealed that there is an existing digital divide among students with different socio-economic status. A huge percentage of the studying population in the country encounter problems and challenges in acquiring digital devices for their online classes. If one does not have the device, then their exposure to software to applications is compromised as well.

Table 4. Comparison on the Level of Exposure in Downloading and Using Software Applications among Respondents

Respondents	Percentile			Mean Rank
	25th	Median	75th	
Students	3.00	3.38	3.85	718.81^{A}
Faculty Member	3.23	3.85	4.38	971.79 ^{B}
Administrative Staff	3.15	3.69	4.54	935.13 ^{B}

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

Difference in the Level on Cybersecurity Knowledge among the Respondents

Table 5 shows that there was a statistically significant difference in the level of knowledge in cybersecurity policies among the different groups of respondents, $H_{(2)} = 9.455$, $p < 0.001$. Specifically, students had significantly lower cybersecurity knowledge compared to faculty members and administrative staff. Meanwhile, the level of cybersecurity knowledge between faculty members and administrative staff are not significantly different. Al-Janabi, & Al-Shourbaji (2016) observed a contradicting finding with the present study. In their study, they revealed that researchers, undergraduate students, and employees within educational environments in different countries in the Middle East, do not have the necessary knowledge and understanding of the importance of information security principles and their practical application in their daily work. The test of difference further showed that their knowledge is not significantly different. However, as regards the relatively lower knowledge of students, Scott-Hayward (2015) concluded that the awareness of cybersecurity is very low among students and is often unaware of many aspects of computer crime. Based on the previous table, students have shown significantly lower exposure to software applications. This explains the finding that students have lower knowledge on cybersecurity. The limited experience of the students on the use of technology may have contributed to their level of knowledge on cybersecurity.

Moreover, the results in Table 6 reveal that there was a statistically significant difference in the level of cybersecurity knowledge among the respondents along System and Data Access and control, $H_{(2)} = 39.390$, $p < 0.001$. Specifically, the Dunn-Bonferroni post hoc test results showed that the cybersecurity knowledge of the different groups of respondents are significantly different from each other with the students having the lowest while the administrative staff had the highest. One of the reasons could be the little experience and exposure of the students to cybersecurity issues as compared to the faculty members and administrative staff. This is because according to Aldawood et.al, (2020) teachers and admin staff with little exposure to cybersecurity issues tend to have surface knowledge in cybersecurity.

In terms of Communications and Email Policy, there was significant difference in the level of knowledge among the different respondents, H $_{(2)}$ = 21.796, p < 0.001. Specifically, the awareness level of the administrative staff is significantly higher than the students and faculty members. However, there was no significant difference in the level of knowledge between students and faculty members. The higher knowledge among administrative staff may be accounted to the initial training on cybersecurity which have been conducted among administrative staff in the university. As a support to this claim, Pancheva (2020) explained that the trainings received by school staff as skeleton forces during the pandemic influenced their awareness on safe cybersecurity practices. Thus, they manifest higher knowledge on the different aspects, activities and effects of cybersecurity.

Meanwhile, there were also statistically significant differences in the knowledge level among the different groups of respondents in line with Acceptable Use Policy (H $_{(2)}$ = 40.864, p < 0.001) and password/passphrase policy (H $_{(2)}$ = 33.857, p < 0.001). Specifically, students had significantly lower cybersecurity knowledge compared to faculty and administrative staff. Meanwhile, the level of cybersecurity knowledge between faculty members and administrative staff are not significantly different. Such finding implies that students need more knowledge on using or setting strong password containing alphanumeric with symbols. Also, it connotes that they are not yet fully aware of the downside of setting their password using their personal information. This finding is explained by Gärdekrans (2017) in his study of password practices of college learners. He mentioned that the value that the students put towards anything that is supposed to be protected influence their password practices. It is interesting that many from the surveyed students have not shown high regard in protecting their local school accounts by using strong passwords.

Furthermore, the result showed that there was no significant difference in the level of cybersecurity knowledge in Backup Policy among the different groups of respondents, H $_{(2)}$ = 4.218, p = 0.121. In short, students, faculty members and administrative staff show the same knowledge on backup policy. There are no existing published studies that focused on knowledge of the academic community on backup policies. However, as regards information security, in general, Marks & Rezgui (2009) have shown equal knowledge level among the members of the academic community. The authors explained that regular and frequent orientation and forums conducted among the surveyed respondents may have caused the equal level of knowledge.

In terms of Wireless Policy, Network Security, and Website Policy, there was significant difference in the level of knowledge among the different respondents, H $_{(2)}$ = 26.280, p < 0.001. Specifically, the awareness level of the administrative staff is significantly higher than those of the students and faculty members. However, there was no significant difference in the level of knowledge between students and faculty member. This may again be attributed to the training for which the administrative staff have initially undertaken along cybersecurity (Pancheva, 2020).

In line with Storage Device, Mobile Device, Bring Your Own Device Policy, there was significant difference in the level of knowledge among the different groups of respondents, $H_{(2)}$ = 18.205, p < 0.001. The level of knowledge of the students is significantly lower than those of the administrative staff but is not significantly different with faculty members. Moreover, the level of knowledge between faculty members and administrative staff was not significantly different. This finding is consistent with the data of Afreen (2014) who noticed that students have lower awareness on BYOD policies than teachers. The author explained that this is due to the nature of work of teachers. Since teachers are more immersed in the operation of the school, they tend to become more aware of these policies.

Table 5. Comparison of the Level on Cybersecurity Knowledge Among the Respondents

Dimensions of Cybersecurity Knowledge		Percentile			Mean Rank
		25th	Median	75th	
System and Data Access and Control Policy					
	Students	3.00	3.42	3.83	740.72^{A}
	Faculty Member	3.00	3.58	4.00	832.71 ^{B}
	Administrative Staff	3.17	3.75	4.00	954.17 C
Communications and Email Policy					
	Students	3.00	3.55	3.91	753.68^{A}
	Faculty Member	3.00	3.64	4.00	793.97^{A}
	Administrative Staff	3.09	3.82	4.00	918.28 ^{B}
Acceptable Use Policy					
	Students	3.00	3.56	4.00	738.77^{A}
	Faculty Member	3.00	3.89	4.00	856.66 ^{B}
	Administrative Staff	3.11	4.00	4.00	937.70 ^{B}
Password/Passphrase Policy					
	Students	3.00	3.50	4.00	742.57^{A}
	Faculty Member	3.00	3.83	4.00	845.67 ^{B}
	Administrative Staff	3.25	4.00	4.00	926.71 ^{B}
Backup Policy					
	Students	3.00	3.67	4.00	768.73^{A}
	Faculty Member	3.00	4.00	4.00	781.12^{A}
	Administrative Staff	3.00	4.00	4.00	837.76^{A}
Wireless Policy, Network Security, and Website Policy					
	Students	3.00	3.67	4.00	750.73^{A}
	Faculty Member	3.00	3.89	4.00	803.59^{A}
	Administrative Staff	3.44	4.00	4.00	925.47 ^{B}
Storage Device, Mobile Device, Bring Your Own Device Policy					
	Students	3.00	3.40	4.00	752.87^{A}
	Faculty Member	3.00	3.50	4.00	817.50^{AB}
	Administrative Staff	3.00	3.90	4.00	894.98 ^{B}
Overall Policy					
	Students	3.03	3.51	3.85	739.52
	Faculty Member	3.00	3.67	4.00	843.28
	Administrative Staff	3.09	3.83	4.00	949.11

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

Conclusion and Recommendations

The members of the academic community of Cagayan State University (CSU) are well informed about the aspects, importance and effects of cybersecurity. Such awareness is translated into positive cybersecurity practices which may have reduced their exposure to cybercrimes. Among members of the CSU academic community, the students need more improvement on cybersecurity knowledge as compared to the faculty members and administrative staff. Hence, much is desired to capacitate them through the proposed cybersecurity policy. It is also recommended that the CSU management should maintain the high cybersecurity knowledge of the faculty members and administrative staff through continuing professional development on cybercrimes as this is possible instrument to lessen their exposure to cybercrimes. Additionally, cybercrime topics must be included as part of syllabus in ethics and basic computer courses among those who are enrolled in all programs. 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

Afreen, R. (2014). Bring your own device (BYOD) in higher education: Opportunities and challenges. International Journal of Emerging Trends & Technology in Computer Science, 3(1), 233-236.

Akçayır, G. (2017). Why do faculty members use or not use social networking sites for education?. Computers in human behavior, 71, 378-385.

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.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences, 10(10), 3660.

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.

Arrosagaray, M., González-Peiteado, M., Pino-Juste, M., & Rodríguez-López, B. (2019). A comparative study of Spanish adult students' attitudes to ICT in classroom, blended and distance language learning modes. Computers & Education, 134, 31-40.

de los Santos, G. E., & Rosser, W. (2020). COVID-19 shines a spotlight on the digital divide. Change: The Magazine of Higher Learning, 53(1), 22-25.

Gärdekrans, R. (2017). Password Behaviour: A Study in Cultural and Gender Differences.

Geers, K. (2011). Strategic cyber security. Kenneth Geers.

Gonzales, R. H. (2014, March). Social media as a channel and its implications on cyber bullying. In DLSU Research Congress.

Heffron, J. K. C. (2014). The Philippine cybercrime prevention act of 2012: To protect or destroy. DLSU Business & Economics Review, 24(1), 96-103.

Husák, M., Bartoš, V., Sokol, P., & Gajdoš, A. (2021). Predictive methods in cyber defense: Current experience and research challenges. Future Generation Computer Systems, 115, 517-530.

Jacobs-Israel, M., & Moorefield-Lang, H. (2013). Redefining technology in libraries and schools: AASL best apps, best websites, and the SAMR model. Teacher Librarian, 41(2), 16.

Marks, A., & Rezgui, Y. (2009, September). A comparative study of information security awareness in higher education based on the concept of design theorizing. In 2009 International

Conference on Management and Service Science (pp. 1-7). IEEE.

Nozaleda, B. M. (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 (TURCOMAT), 12(11), 3256-3262.

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2022). BYOD policy compliance: Risks and strategies in organizations. Journal of Computer Information Systems, 62(1), 61-72.

Pan, C., Zhong, W., & Mei, S. (2015). Finding the weakest link in the interdependent security chain using the analytic hierarchy process. Journal of Advances in Computer Networks, 3(4), 320-325.

Quantitativa, D. D. P. (2007). An overview of research designs relevant to nursing: Part 1: quantitative research designs. Rev Latino-am Enfermagem, 15(3), 502-7.

Schneider, E. J. (2021). From saving face to saving lies: prioritizing the public in public relations (Doctoral dissertation, University of Missouri--Columbia).

Scott-Hayward, S., Natarajan, S., & Sezer, S. (2015). A survey of security in software defined networks. IEEE Communications Surveys & Tutorials, 18(1), 623-654.

Senthilkumar, K., & Easwaramoorthy, S. (2017, November). A Survey on Cyber Security awareness among college students in Tamil Nadu. In IOP Conference Series: Materials Science and Engineering (Vol. 263, No. 4, p. 042043). IOP Publishing.

Yogesh Hole et al 2019 J. Phys.: Conf. Ser. 1362 012121