[1] **Joselle D. Concepcion**

[2] **Thelma D. Palaoag**

An Assessment of Cybersecurity Awareness among Academic Employees at Quirino State University: Promoting Cyber Hygiene

Journal of Electrical Systems

Abstract: - With the ever-changing and increasing dependence on technology, employee behavior poses a significant cybersecurity risk, and the education sector is no exception. To secure sensitive information and ensure educational activities, enhancing cybersecurity awareness among academic employees is vital. This study aimed to assess cybersecurity awareness at Quirino State University. An online questionnaire survey was presented to employees to assess their comprehension of cybersecurity and adherence to existing rules and procedures. The survey results were examined to establish the level of cybersecurity awareness and opportunities for development. While the majority of academic personnel had a basic awareness of cybersecurity, there were still areas for development, such as the risk of device threats. The findings of this study hold significant implications for the education sector, emphasizing the need for a comprehensive approach to cybersecurity awareness. This approach includes regular training sessions, the establishment of effective policies, and the integration of technology-based solutions. By implementing such measures, the university can foster a proactive defense strategy and create a safer digital landscape for the entire institution, promoting a culture of cyber hygiene among its employees.

Keywords: Cybersecurity Awareness, Cyber Threats, Employees, Higher Education.

I. INTRODUCTION

As cyber threats continue to grow, the need to protect our data and information becomes even more crucial. Each day, we working individuals make decisions that can have a substantial influence over the safeguarding of an institution's valuable data resources. From opening an e-mail attachment to clicking on a website link to permitting an unauthorized person into restricted areas, these choices can potentially lead to negative repercussions [1]. To establish strong cyber security, the people, processes, and technology in an institution must all work in tandem [2]. It has been observed that employees can sometimes be perceived as the weak link within an organization, irrespective of its size or scale [3]. One of the potential risks associated with cyber security is the possibility of human error. This occurs when an employee unintentionally creates a vulnerability that can be exploited by attackers or unknowingly exposes themselves to personal harm [4]. Throughout the course of the pandemic, it is worth noting that the Philippines experienced a rather alarming surge of 200% in the number of phishing incidents. In June 2020, unfortunately, there were instances where certain university student portals experienced security breaches. These incidents resulted in the unauthorized access to the personal information of a significant number of students, which is indeed concerning. Due to a recent increase in incidents occurring within universities, the National Privacy Commission has taken the initiative to create a code of conduct specifically tailored for the education sector. Additionally, they are also working on providing guidance on how to effectively handle data security breaches [5].

In order to minimize the risk of falling prey to cybercrime, it is crucial for individuals to remain vigilant and prioritize their own security and safety procedures [6]. Furthermore, it is worth noting that institutions are recognizing the importance of investing in professional training programs for their employees. This proactive approach serves as a crucial risk mitigation policy as it aims to enhance their understanding of cyber threats and the corresponding defenses [7]. Cyber hygiene involves adopting cybersecurity procedures to protect personal information on internet-connected devices. Employees' specific behaviors may differ depending on their responsibilities, the type of company for which they work, and the industry the institution is in [8]. An effective cyber security awareness program should contain appropriate training aligned with the goals of the institution, with a focus on increasing cyber security awareness when performing employee activities, and communication processes across all stakeholders about any cyber security problems [9]. Organizations may improve their overall cyber

[1] Quirino State University, Diffun, Quirino, Philippines. joselledcconcepcion@gmail.com

[2] University of the Cordilleras, Baguio, Philippines. tpalaoag@gmail.com

Copyright © JES 2024 on-line : journal.esrgroups.org

resilience and protect sensitive information by implementing cyber hygiene practices and cultivating a culture of cybersecurity awareness.

Being the only university in the province of Quirino, adapting to digital advancements while simultaneously establishing a cyber-resilient atmosphere is challenging. As a young university, the adoption and implementation of cyber security processes are not so comprehensive, although there are existing policies addressing data privacy and the university has a designated data privacy officer. Thus, the objective of this study is to assess the level of cybersecurity of Qurino State University employees', specifically to evaluate their awareness in the areas of (a) operational security, (b) device security, and (c) account security, and to assess their willingness to learn more about cybersecurity. The goal of this research is to better understand academic employees' existing cybersecurity understanding and practices as well as suggest areas for development. The findings of this survey will give significant insights into the existing state of cybersecurity knowledge among academic employees and may be used for cyber hygiene promotion strategies. This study's findings will be useful not just for Quirino State University but also for other academic institutions in strengthening their cybersecurity awareness initiatives.

II. METHODOLOGY

The researchers employed a quantitative data collection methodology that closely resembled the approach used in the data collection and analysis described in references [10] and [11]. The study's respondents were comprised of employees of Quirino State University. The survey questions employed in this study were derived and adjusted from the Ford Foundation Cyber Security Assessment Tool and a previous study on cyber security awareness [11]. The questionnaire is divided into two sections. The first section focuses on gathering demographic information, such as your name, age, sex, and highest level of education completed. In the second section, we delve into the topic of cyber security awareness. This part focuses on various aspects such as operational, device, and account security. The data was inputted and extracted in IBM Statistical Package for the Social Sciences software, which helped in assessing the data. In this study, statistical tests such as frequency and mean were employed to analyze the data.

A. Instrument Design

The questionnaire underwent evaluation and validation by a group of IT experts to ensure its reliability and validity. Based on our research methodology, we distributed a total of 217 questionnaires for our study. We aimed to achieve a confidence level of 99% with a margin of error of 5%. This sample size was determined using the Raosoft formula, which takes into account the population size of 500. The questionnaire link was produced in Google Forms and emailed to the respondents. The researchers assessed respondents' cyber security knowledge using a 4-point Likert scale, as shown in Table 1. The descriptive rating for mean and grand mean is presented in Table 2.

Table 1. Likert Measurement Scale

Adjectival Rating	Scale
Strongly Agree	4
Agree	3
Disagree	2
Strongly Disagree	1

Table 2. Descriptive rating

Adjectival Rating for Mean	Adjectival Rating for Grand Mean	Mean Range
Strongly Agree	High	3.26-4.00
Agree	Moderate	2.51-3.25
Disagree	Low	1.76-2.50
Strongly Disagree	Very Low	1.00-1.75

III. RESULTS, DISCUSSIONS AND CONCLUSION

B. Respondents

The distribution of the respondent's profile is broken down into three sections: age, sex, and highest educational attainment. Based on the data gathered under the age of respondents, out of 217 respondents, 57, or 26.27%, are 41 years old or older, which is the lowest number, and 76, or 35.02%, are from the age of 21 up to 30. The majority of respondents (84, or 38.71%) are between the ages of 31 and 40. The distribution also found that the majority of respondents are female (73.27%, or 159 out of 217 respondents), with males comprising 58, or 26.73%.
Moreover, the majority of respondents are master's degree holders, accounting for 109, or 50.23%, of the total number of respondents. On the other hand, 23.50%, or 26 out of 217 respondents, have a doctoral degree, while the remaining 82, or 37.79%, are bachelor's degree holders.

C. Awareness on Operational Security

Operational is a component of a business process that is essential for the company to perform efficiently in order to continue running. It often involves action by people, normally within the organization [12]. Operational security (OPSEC) is a crucial aspect of risk management and security protocols. Its primary objective is to safeguard sensitive information from unauthorized access or potential compromise [13].

Table 3. Mean Distribution of the Level of Awareness along Operational Security

Operational Security	Mean	Descriptive Rating
I only entertain visitors with proper ID or when I recognize them.	2.80	Agree
I shred printed information for disposal.	3.18	Agree
I do not use my personal devices and personal email accounts when communicating within the organization.	1.61	Strongly Disagree
I only release internal documents when they are legally requested.	2.56	Agree
Grand Mean	2.53	Moderate

The results indicate that the employees have a moderate level of awareness of operational security practices, as shown in Table 4, with a grand mean of 2.53. Information can be obtained from printed information if it is not properly disposed [14]. Majority of the employees dispose of printed information by shredding. This indicates that there is an existing policy for the disposal of printed information, which suggests that the organization is taking measures to maintain the confidentiality of sensitive information. However, the employees have a low degree of awareness regarding the use of personal devices and email accounts when communicating within the organization, with a mean value of 1.61. Personal devices have become the most attractive target for attackers to collect sensitive user and company data because they are widely used for a variety of tasks. Cybercriminals can use this information for blackmail or financial gain [15]. To prevent the inadvertent or unintended exposure of classified or sensitive data, it is important to have an effective operational security program [13]

D. Awareness on Device Security

Device security meant to secure sensitive information stored on and transferred by portable devices as well as the network to which the devices are connected [16].

Table 4. Mean Distribution of the Level of Awareness along Device Security

Device Security	Mean	Descriptive Rating
I do not use my personal email for work-related tasks	2.08	Disagree
I do not download pirated personal or work-related software	1.99	Disagree
I encrypt backups and/or external media (hard drives, flash drives, etc.)	2.66	Agree
I have an updated operating system, software, and anti-virus on my devices (computer, phone, etc.)	2.60	Agree
Grand Mean	2.33	Low

The findings indicate that the employees exhibit a relatively low level of awareness on device security practices with a grand mean of 2.33. It demonstrates that the majority are aware of securing their devices such as software

update and backups, yet engage in activities that can lead to device vulnerability such as using personal email for work-related tasks and downloading pirated software. According to the US Federal Trade Commission (FTC), allowing workers to use personal email for work creates substantial dangers of IP theft, loss of company privacy or violation of consumer privacy, and disruption of network operations. It can also result in a data loss incident or breach [17].

The results of our study, which show that employees agree that they download pirated software for personal or work-related use, make it clear that some people may not fully understand the legal ramifications of software piracy or may underestimate the risks involved [18]. Also, there are numerous risks associated with accessing digital piracy websites, including the hidden danger of virus/malware or downloaded files [19]. This virus/malware can infect your device or compromise the network.

The awareness of mobile users to threats is an important part of cyber security since the skills necessary from a mobile user to engage safely with his/her smartphone differ from those required for responsible and safe PC use [20]. By educating employees on the dangers of using personal email for work and downloading pirated software, they can make informed decisions and take necessary steps to safe-guard their devices and the network from potential cyber threats.

E. Awareness on Account Security

A data breach might imply a variety of things. In essence, it indicates that data has been accessed by unauthorized individuals, which they should never have had access to it. It also implies that data account protection has failed. Personal details, email exchanges, online transactions, and financial records can all be represented by the data [21].

Table 5. Mean Distribution of the Level of Awareness along Account Security

Account Security	Mean	Descriptive Rating
I am using a password manager app to store existing passwords	3.51	Strongly Agree
I am using two-factor/multifactor authentication when I log in to my e-mail or apps (ex. Google authenticator, OTP, etc.)	3.58	Strongly Agree
I do not share my credential information such as name, date of birth, age, credit card number, and others when I receive email or SMS that demands it	3.72	Strongly Agree
I use VPN when connecting to a public network	2.77	Agree
I do not open links in emails from unknown senders or unfamiliar websites	3.58	Strongly Agree
I do not connect to open Wi-Fi networks in public places	2.81	Agree
Grand Mean	3.32	High

The results suggest that workers have high awareness of account security policies, with a grand mean value of 3.32. Employees highly support the usage of password managers, two-factor/multifactor authentication, and the refraining from revealing personal information when receiving emails or text messages from unknown sources. Additionally, employees recognize the importance of utilizing VPN while connecting to public networks and to avoiding connecting to public Wi-Fi networks.

Employees' high degree of account security awareness benefits the institution by minimizing the occurrence of data breaches. By reinforcing these behaviors, employees help to safeguard and protect the digital environment of the institution.

F. Willingness to learn more about Cyber Security

Improving knowledge on cyber risks is one step important stakeholders should take to defend such organizations from developing cybersecurity vulnerabilities [22]. The purpose of awareness is to engage and motivate the audience and to gently remind them of the expectations placed upon them. [23].

Table 6. Mean Distribution of the Willingness to Learn about Cyber Security

Willingness to learn more about cyber security	Mean	Descriptive Rating
I would like to attend training regarding cyber security awareness	3.66	Strongly Agree

I want to learn more about cyber security	3.77	Strongly Agree
Grand Mean	3.72	High

A grand mean score of 3.72 and a descriptive rating of "High" imply that the majority of employees are eager to learn more about cybersecurity. It means that workers are keen to attend cybersecurity trainings that will benefit both the employees and the organization as a whole.

G. Implications of Results

This study highlights the importance of increasing cybersecurity awareness among academic employees at Quirino State University. Our study also found a consistent pattern of low cybersecurity awareness among employees, particularly in terms of device security practices, in alignment with prior research conducted by [24]. It was found that employees lack awareness regarding the potential risks that come with using smartphones. It may risk the confidentiality and integrity of sensitive information or compromise the security of the network.

In a digital academic landscape, it is crucial to address vulnerabilities and protect against cyber threats. A cybersecurity breach could disrupt administrative functions and teaching, with significant consequences. Cybersecurity incidents can damage the institution's reputation and erode trust among students, parents, and other stakeholders.

In order to address these potential threats and strengthen the cybersecurity posture of the organization, it is evident that a collaborative and focused approach is necessary. According to the data in Table 6, which highlights their expressed interest in learning more about cybersecurity, it is essential to develop and implement a comprehensive cybersecurity awareness program for academic personnel. This program has the potential to significantly contribute to enhancing employees' knowledge and comprehension of cyber threats.

The significance of a cybersecurity program in safeguarding internet users from cyberattacks and growing cyber dangers is reinforced by the insights obtained from prior research [23]. As the institution grows, it is important to place emphasis on and allocate resources towards cybersecurity education and initiatives. This is necessary not just to protect the institution but also to cultivate a culture of cyber hygiene and awareness among the academic community.

H. Challenges, Opportunities, and Recommendations

One of the challenges is limited resources and competing priorities. However, opportunities exist for addressing these challenges. Customized and engaging training programs tailored to the unique needs of academic employees can improve awareness and compliance. Collaboration between academic departments and IT departments is vital to building a culture of cybersecurity awareness and aligning academic goals with security measures. By utilizing technology-driven solutions, such as mobile applications or interactive self-learning platforms, the potential arises for continuous awareness campaigns that can effectively engage a wide-ranging audience, eliminating the necessity for in-person meetings or seminars.

Relevant studies in the field have shown promising results. For instance, a study [26] observed a significant improvement in employees' cybersecurity awareness following the implementation of knowledge transfer and targeted training sessions focused on cybersecurity. Another study [27] established a positive correlation between organizational policies, employee behavior, training initiatives, IT knowledge, and education, all contributing to heightened security awareness and practices among employees. The results of their studies indicate that employees possess a considerable level of cybersecurity and account security awareness when they receive suitable training and education. Additionally, organizational policies and behaviors that prioritize security awareness contribute to this heightened level of awareness among employees.

I. Areas for Further Research

This study establishes a foundation for future research efforts. In order to obtain a more comprehensive understanding, future research endeavors may explore the efficacy of diverse training approaches in enhancing cybersecurity awareness and influencing behavioral patterns among academic personnel. It is essential to understand the approaches that result in the most significant impact. Furthermore, it would be beneficial to do further study on the practical implementation of cyber hygiene practices among academic personnel and their effectiveness in reducing cybersecurity vulnerabilities. Conducting comparative analyses with other universities or educational institutions might yield significant benchmarks and insights pertaining to ideal practices. Through

persistent exploration of these domains, we may effectively modify and develop cybersecurity protocols to effectively counter the ever-changing threats in the online environment.

IV. CONCLUSION

Based on the findings of this research study, it can be inferred that the general level of cybersecurity awareness among academic employees at Quirino State University is moderate, highlighting potential areas for enhancement. The findings emphasize the significant importance of ongoing education and training in enhancing the organization's cybersecurity posture.

The significance of these findings has implications for the wider education sector, emphasizing the necessity of adopting a comprehensive approach to improving cybersecurity awareness. Additional investigation is crucial in order to explore more comprehensively the particular problems and prospects associated with enhancing cybersecurity awareness and advocating for cyber hygiene among academic personnel.

In conclusion, it is essential to establish a cybersecurity culture within educational institutions in order to safeguard sensitive data and information, reduce cyber threats, and strengthen the resilience of academic activities in a constantly changing digital landscape.

REFERENCES

[1] Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. International Management Review, 13(1), 37.

[2] Anonymous. (n.d.). What is Cybersecurity? Cisco. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[3] Kemper, G. (2019). Improving employees' cyber security awareness. Computer Fraud & Security, 2019(8), 11-14

[4] Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2018). Insider threat: The human element of cyberrisk. McKinsey Quarterly, 1-8.

[5] Gorriceta, M. (2021, January 29). A brave new world: Cybersecurity in 2021. The Manila Times, https://www.manilatimes.net/2021/01/29/business/columnists-business/a-brave-new-world-cybersecurity-in-2021/834365

[6] 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.

[7] Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, 101827.

[8] Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 128, 113160.

[9] R. Sabillon J. Serra-Ruiz, V. Cavaller and J. J. Cano, "An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada" 2021 Research Anthology on Artificial Intelligence Applications in Security, doi: 0.4018/978-1-7998-7705-9.ch008

[10] Y. Yang *et al.,* "A survey on cyber security awareness among college students in Tamil Nadu," *IOP Conference Series Materials Science and Engineering,* vol 263, no. 4, 2017, Art. No 042043, doi: 10.1088/1757-899X/263/4/042043.

[11] Adamu, A. G., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. International Journal of Electrical and Computer Engineering, 12(1), 572.

[12] Zalewski, T. (2019). An Introduction to Operational Security Risk Management. Xlibris Corporation.

[13] Anonymous (n.d.). *Operational Security (OPSEC).* Fortinet. https://www.fortinet.com/resources/cyberglossary/operational-security.

[14] Ramjist JK, Coburn N, Urbach DR, et al. Disposal of Paper Records Containing Personal Information in Hospitals. JAMA. 2018;319(11):1162–1163. doi:10.1001/jama.2017.21533

[15] M. Morolong, A. Gamundani and F. Bhunu Shava, "Review of Sensitive Data Leakage through Android Applications in a Bring Your Own Device (BYOD) Workplace," 2019 IST-Africa Week Conference (IST-Africa), 2019, pp. 1-8, doi: 10.23919/ISTAFRICA.2019.8764833.

[16] What Is Mobile Device Security? (n.d.). Cisco. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/mobile-device-security.html#~components

[17] Anonymous. (n.d.) Why sending data to your personal email is a risk? Tessian. https://www.tessian.com/blog/the-risks-of-sending-data-to-your-personal-email/

[18] Darryl, A., Seale., Michael, Polakowski., Sherry, Schneider., Sherry, Schneider. (1998). It's not really theft!: Personal and workplace ethics that enable software piracy. Behaviour & Information Technology, 17(1):27-40. doi: 10.1080/014492998119652

[19] Suwa, R. (2021). Detecting Cybersecurity Threats from Online Digital Piracy Websites.

[20] Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. Computers & Security, 73, 266-293.

[21] Impe, K. (2016, October 18). *The Importance Of Account Protection And Incident Response Plans.* Security Intelligence. https://securityintelligence.com/data-breaches-importance-account-protection-incident-response/.

[22] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber security behavior among higher education students in Malaysia," Journal of Information Assurance & Cybersecurity, pp. 1-13, 2017

[23] Tirumala, S. S., Valluri, M. R., & Babu, G. A. (2019, January). A survey on cybersecurity awareness concerns, practices and conceptual measures. In 2019 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

[24] Nisreen, Ameen., Ali, Tarhini., Mahmood, Hussain, Shah., Nnamdi, O., Madichie. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. Computers in Human Behavior, 104:106184-. doi: 10.1016/J.CHB.2019.106184

[25] Rahman, N., Sairi, I., Zizi, N., & Khalid, F. (2020). The importance of cybersecurity education in school. Int. J. Inf. Educ. Technol, 10(5), 378-382.

[26] Hamida, Asker., Abdalmonem, Tamtam. (2020). An Investigation of the Information Security Awareness and Practices among Third Level Education Staff, Case Study in Nalut Libya. European Scientific Journal, ESJ, 16(15):20-20. doi: 10.19044/ESJ.2020.V16N15P20

[27] Ling, Li., Wu, He., Li, Xu., Ivan, K., Ash., Mohd, Anwar., Xiaohong, Yuan. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45:13-24. doi: 10.1016/J.IJINFOMGT.2018.10.017