IBSUniversity Journal of Business and Research
ISSN: 3007-3936 (Online)
Volume 2, Issue 1, June 2025

Evaluating cybersecurity awareness and practices among employees at a private university in Papua New Guinea

Valli Ramamurthy
IBSUniversity, Port Moresby, Papua New Guinea
valli.ramamurthy@ibs.ac.pg

Victor Bogalin
IBSUniversity, Port Moresby, Papua New Guinea
Victor.Bogalin@ibs.ac.pg

Promise Zvavahera
IBSUniversity, Port Moresby, Papua New Guinea
promisezvavahera59@gmail.com

Emmanuel Aquino
Western Pacific University
eaquino@wpu.ac.pg

Abinaya Nagamuthu
IBSUniversity, Papua New Guinea
abinaya.nagamuthu@ibs.ac.pg

Abstract

As organizations increasingly move towards digital transformation, the internet has become their prominent channel of communication and data sharing. This has raised concerns about cybersecurity, compelling organizations, including academic institutions, to strengthen their protection sphere. Employees play a significant role in defending against cyberattacks, and it becomes essential for the security team to constantly raise awareness among them. As part of efforts to enhance cybersecurity, this study assessed the level of cybersecurity awareness among employees at a private university in Papua New Guinea. Data were collected through online questionnaires and structured face-to-face interviews with senior management. Data were analyzed using statistical tools. The findings revealed that only 20% of the employees had high levels of awareness about cybersecurity, indicating the need for more awareness and training to strengthen cybersecurity measures. Employee-related vulnerabilities were identified, including weak password practices, unsafe browsing behaviors, and failure to adhere to established cybersecurity

protocols. It is recommended that the institution provide ongoing cybersecurity training programs to enhance the level of awareness among employees and the degree to which they adhere to acceptable standards. Furthermore, to address typical weaknesses, such as weak passwords and dangerous browsing, it is necessary to develop explicit policies and monitoring procedures. This study contributes to the understanding of human-related cybersecurity risks in higher education institutions, highlighting the need for targeted awareness and policy interventions.

Keywords: Cybersecurity awareness, vulnerabilities, academic institutions, human-related cybersecurity

1. Introduction

In a progressively digitized landscape, cybersecurity has become a paramount concern for all sectors of the economy, including universities. Universities, which frequently handle substantial amounts of sensitive data, including student records, research outputs, and financial and administrative information, have emerged as prime targets for cyber threats across the globe. Although technical measures, such as firewalls and antivirus software, are essential, the significance of human behavior in upholding cybersecurity is paramount. Employees, as regular users of institutional digital systems, significantly influence the robustness or vulnerability of an organisation's cyber defenses (Admass et al. 2023). As noted by Tolossa (2023), employee cybersecurity awareness is crucial for managing and minimizing risks related to cyberattacks, including phishing, malware, ransomware, and data breaches. Despite the increasing global focus on cybersecurity training and education, most institutions, especially in developing countries like Papua New Guinea, may be lacking resources or strategic frameworks necessary to guarantee sufficient awareness and preparedness among their employees.

This study aims to evaluate the level of cybersecurity awareness among employees at a private university, including their perceptions of best practices and their ability to recognize and respond to potential cyber threats. By examining these aspects, the study seeks to identify gaps in awareness and recommend strategies to strengthen cybersecurity resilience within the university environment. The study sought to answer this research question: To what extent are employees at a private university in Papua New Guinea aware of cybersecurity threats, and how effectively do they adhere to cybersecurity best practices? To answer this question, the following objectives were developed:

i) evaluate the current level of cybersecurity knowledge and awareness among university employees by gender and age.
ii) identify and discuss common cybersecurity threats encountered by employees in their daily work environment.
iii) examine employees' attitudes and practices towards cybersecurity protocols and policies.
iv) recommend strategies for enhancing cybersecurity awareness and training initiatives within the university.

The subsequent sections will present the theoretical framework underpinning the study, literature review, the methodology, findings and discussion, conclusions, and implications for policy and practice.

2. Theoretical Framework: Protection motivation theory

This study is grounded in the protection motivation theory (PMT) established by Rogers (1975), which offers a comprehensive framework for analysing individuals' behavioural reactions to perceived threats. PMT is extensively utilised in information security research to explain how individuals evaluate threats and determine whether to adopt preventive actions, such as adhering to cybersecurity protocols or participating in awareness training. PMT posits that an individual's motivation to engage in protective behaviours is shaped by two cognitive processes: risk assessment and coping appraisal.

Threat evaluation is assessing the perceived severity of a cyber threat and an individual's susceptibility to it (Shi et al., 2019). In the university setting, this pertains to the seriousness with which employees regard threats such as phishing, malware, or data breaches, and their belief in the potential impact of these threats on their job or institutional operations.

Coping appraisal pertains to the perceived effectiveness of suggested protective actions (e.g., employing strong passwords, reporting dubious emails) and the individual's self-efficacy regarding their capacity to execute these actions, weighed against the perceived costs or inconveniences associated with adopting such behaviours (Wang et al., 2017). This study, therefore, seeks to evaluate the behaviours and practices of employees in dealing with cyberthreats. The next section of the study discusses literature that is pertinent to the study.

3. Literature review

For all organizations, including educational institutions, to be able to provide their consumers with service that is both of high quality and delivered promptly, digital transformation has become a fundamental requirement. The utilization of digital technologies offers these organizations a variety of advantages, including the expansion of their business networks; yet, at the same time, these technologies also present them with an increased number of cybersecurity concerns (Sonja, 2011). The data report from the IC3 (2023) underscores the fact that the number of cybercrimes that are recorded continues to rise year after year. Compared to 467,361 registered complaints with a loss of 3.5 billion dollars in 2019, it has almost doubled in 5 years of time having 880,418 complaints with a loss of 12 billion dollars. This alarming report emphasizes the importance of cybersecurity for all organizations, and it is particularly pertinent for academic institutions in developing countries like Papua New Guinea.

3.1 Cyberattacks in Universities

The use of digital tools and technologies for teaching and learning and administrative purposes has increased in recent decades, specifically after the COVID-19 pandemic. The COVID-19 lockdown in 2020 and subsequent years has forced more academic institutions to shift to an online mode to continue the teaching and learning process (Cucinotta & Vanelli, 2020). Moreover, most of the universities use learning management systems (LMS), customized Enterprise Resource Planning (ERP), and cloud infrastructure for managing their data and operations. Use of digital tools has increased efficiency and productivity but also exposed universities to different types of threats such as viruses, social engineering attacks, ransomware, and unauthorized data access, compromising confidentiality, availability, and accessibility (Tazi et al., 2023). Itro (2023) reported that educational institutions are the honeypot for attackers as they have a large volume of diverse data. This is corroborated by Jawaid (2022), who highlighted that the cyber breaches in

universities are increasing significantly, highlighting the need for strengthening the cybersecurity sphere.

3.1.1 Employees' awareness of cybersecurity

A study conducted in a South African University by Ntloedibe et al. (2024) indicated that a lack of awareness among staff members was one of the main reasons for security breaches. Human factors such as carelessness, ignorance, and other unintentional activities also add cyber risks (Hadlington, 2017) to universities. It is beneficial for the universities to create adequate awareness among all their users about the existing and the new threat landscape (Shah &Agarwal, 2023). Users with adequate awareness and education will be able to handle cyber incidents better than others (CISA, 2022; MeitY, 2022; NCSC, 2022). Hence, universities must assess the current level of awareness and maintain adequate cybersecurity awareness among their staff, helping them to defend against cyberattacks and mitigate their impacts

Today, universities all over the world rely on accurate data to carry out their daily responsibilities. In addition, for the data to be useful to the business, it must be timely, accurate, comprehensive, valid, consistent, and relevant (Faroukhi et al., 2020). But data privacy and confidentiality are heavily impacted by rising numbers of data leaks and unauthorized access. Universities that are exposed to data leak incidents need to face the penalties imposed by the government in addition to their financial and reputation loss (Kamiya et al., 2021).

It is stated that more data leakage and loss of sensitive data like personally identifiable information, personal security information, and personal health information are growing higher due to employees with inadequate awareness. Additionally, how employees behave and what they do with the security aspect is unpredictable, making them the drivers for threats. A study conducted with 214 participants revealed three important facts i) half of the staff had not undergone training ii) more than 60% of staff are not aware of their IT security policies and procedures and iii) 60% of their violations (Fosoh & Amaechi, 2022), which might pose cyber threats are not addressed as per legal requirements. This study results sample the current state of cybersecurity awareness among employees and the reasons why they are the weakest link in the protection sphere.

Security breaches mostly cause a higher impact on the organization's assets and reputation. The average cost of loss incurred is about 3.86 million per cyber incident (SANS, 2023). Compared to this cost, investments for training and awareness programs are lower. While pointing out lack of budget as one of the constraints for effective training, research by Kemper (2019) highlighted that top-level management is getting frustrated by seeing their efforts, time, and cost are not yielding high productivity towards increasing awareness among its staff. Training should be imparted to higher-level and middle-level management staff in addition to technical and operational-level staff. Lack of training and awareness in senior management roles place universities more at risk. Interesting research which studied the relationship of immediate workgroup (IW) such as supervisor behavior and his fellow staff, concluded that if IW adheres to the security practices, then there is a high chance for its team members to follow those safety measures. They are greatly influenced by their workgroup even though there are variations in individual personality traits (Akers, 2017). Therefore, training partners need to consider this relationship and coherence behavior while conducting education and awareness programs.

Universities are imposing more restrictions to impose security, which includes disabled USB ports, blocking social media apps, and turning off features on desktops. However, a study with 25 top global organizations revealed that these companies face complications due to the

interconnected nature of business and increased online data transactions (Kaplan, 2015). Further, hackers gather information from social sites about a specific organization and execute their phishing attack mostly by exploiting weaknesses in the human system. Availability of online tools and apps to hack and crack, either as paid or free tools, makes hacking easy, efficient, and fast. There are several reasons for hacking, such as financial gain, unhappy employees, ex-employees forced into termination, and fun and challenge motivations. Irrespective of the reasons for hacking, employees are again the most targeted victims (Azinheira et al., 2023). Most of these attackers use vulnerabilities in hardware, operating systems, network, and application, and human errors to initiate their attacks. Opening downloaded attachments without scanning, using flash drives and other external storage without protection practices, downloading apps from untrusted sites, and other reasons make malicious code get installed in the systems. Employees should be made aware that hackers will be able to get access to sensitive and confidential data, like user passwords and credentials, using automatic tools. The loss of sensitive and confidential data causes heavy losses to individuals and organizations. Recent research articles support the above arguments and confirm that false apps, banking Trojans designed for mobiles, are used to get access to credentials. The alarming growth of cyber incidents forces the government bodies, business entities, and academic institutions to invest more in strengthening their cybersecurity and raising their employees' awareness (Sophos, 2022). Even though advanced tools and techniques are used for strengthening protection, employees' education and training are the most needed aspects for all organizations.

Over one third of the cybersecurity team argued that creating employee awareness through education and training is more critical than spending on improving infrastructure to protect the network and host from attacks. On the other hand, overexposure and more emphasis on cybersecurity practices might also create a negative impact on organizational security. Sometimes, it leads to cybersecurity fatigue factors such as aversion and disengagement due to cognitive and attitudinal reasons (Reeves et al., 2021). Another important factor to be considered in the employee aspect is optimum bias. It is a cognitive factor that makes employees underestimate threats and thereby increase the success of attacks.

In the era of AI and IoT, organizations are restructuring their operations in a smart environment. IoT is the process of connecting physical systems with the Internet to increase efficiency and productivity (Chugh & Taqa, 2019). IoT devices place more employees on the internet platform. Employees who are overstaying on the internet and cyber loafing are more vulnerable sectors in organizations. Beyond placing their data in cyber risks, they also put their organizations' assets at more risk Hadlington (2017). Creating awareness about new risks among employees will help organizations mitigate the impact of cyber threats.

According to the report of SANS Institute (2023), human vulnerabilities approximately lead to 70% of security breaches and subsequently reveal that training them with adequate skills to identify and protect against threats is a critical need for organizations. A study that explored the role of gender in the context of cybersecurity identified significant variations between male and female staff members. The awareness level is higher among female members than their male colleagues (Daengsi et al., 2022). According to Li et al. (2019), employees with adequate awareness and knowledge about organizational policies could protect and handle cyber threats better than others. Even though female employees are more cautious of cyber threats, their self-efficacy is lower than male employees, which might be increasing the vulnerability of cyberattacks towards them (Anwar et al., 2017). The security framework of the organizations also impacts the ability of employees to handle cyber incidents in an effective way (Li et al., 2019). Hence,

imparting training in a customized way based on their computer skills, cues to action, self-efficacy and self-reporting, and other traits will be more productive than generic training.

4. Research methodology

This study employed a case study approach within a mixed-methods research framework, focusing on a private university in Papua New Guinea. This methodology enabled an in-depth exploration of the institution, allowing for a focused investigation and the generation of detailed insights into cybersecurity awareness and existing vulnerabilities at the university.

At the time of the study, the institution had a total workforce of 150 employees. A purposive sample of 90 staff members comprising both academic and administrative staff whose roles involved regular computer use was selected to participate. Of those invited, 52 individuals completed the survey, yielding a response rate of 58%. To augment the questionnaire data and derive deeper insights from a leadership perspective, in-person interviews were conducted with key individuals, including:

- Heads of Schools;
- Information and Communications Technology Manager;
- Pro-Vice Chancellor;
- Quality Assurance; and
- Representative of the Student Services Department.

The interviews aimed to acquire an in-depth understanding of cybersecurity challenges from a managerial perspective and to corroborate conclusions derived from the questionnaire.

4.1 Data collection and analysis

An online survey was conducted to collect quantitative data from general employees belonging to various departments. The same questionnaire was also used to conduct structured interviews for gathering qualitative insights from managers. The questionnaire was pretested on a different group to ensure clarity, relevancy, consistency, and logical sequence in the order of questions. The feedback obtained assisted in improving the instrument.

In addition to the collected data, existing ICT and security policies, including email policies, password management procedures, backup protocols, and user policies, were reviewed to identify areas of gaps.

4.2 Ethical considerations

Ethical issues were adhered to, respecting the privacy and confidentiality of the participants. No personally identifying information, such as an email address, a name, or a cell phone number, was included in the data that was collected for the study. In addition, participants were provided with sufficient information, which included the aim of the research, the necessity of maintaining confidentiality, and the anonymity of their responses. The questionnaire, permission form, research purpose, and research methodology were all approved by the ethics committee of the university. The study was conducted according to established ethical guidelines. The next section discuss the findings of the study.

5. Findings and discussion

The findings of this study were presented using the objectives of the study, the conceptual framework, and the themes that emerged during data gathering. SPSS was used to analyse quantitative data.

5.1 Demographic statistics

Table 1 below shows details such as age, gender, educational qualifications, and years of experience of the respondents.

Table 1: Demographic data about the respondents

Variables	Category	Count	Percentage
Age	Below 25 years	14	27
	26 to 35 Years	22	42
	36 to 45 years	7	14
	46 to 55 Years	8	15
	55 and above	1	2
Total		52	100
Gender	Male	32	62
	Female	20	38
Total		52	100
Education	Certificate	14	27
	Diploma/Advance Diploma	8	15
	Bachelor	17	33
	Master's and above	12	23
	Doctorate	1	2
Total		52	100
Number of Years Experience	Less than 5 Years	29	55
	6 to 10 Years	6	12
	11 to 15 Years	5	9
	16 to 20 years	6	12
	Above 20 years	6	12
Total		**52**	**100**

Source: Field data

The age distribution shows that most respondents are relatively young, with 69% aged below 35 years. This suggests that a significant portion of the university workforce likely belongs to a generation that has grown up with digital technologies, which could imply a higher baseline familiarity with digital tools, but not necessarily a proportional awareness of cybersecurity threats.

In terms of gender, 62% of respondents are male, and 38% are female. While this ratio does not directly determine cybersecurity awareness, it is important to explore whether gender-

related differences exist in access to training, risk perception, or adherence to cybersecurity protocols.

The education levels are varied, with 33% holding bachelor's degrees, and 25% holding postgraduate qualifications (master's and doctorate combined). This diversity suggests that a substantial number of the employees have formal education that could include or be complemented by digital literacy training. However, the 27% with only certificate-level education may represent a group needing more targeted awareness programs, especially if their roles involve handling sensitive digital information.

Regarding work experience, over half of the respondents (55%) have less than 5 years of experience at the university. This could suggest a relatively new or transitioning workforce that may not yet be fully immersed in institutional cybersecurity culture or policies. Meanwhile, only 21% have more than 15 years of experience, indicating a potential gap in institutional memory and cybersecurity knowledge transfer across generations of staff.

Objective 1: Evaluate the current level of cybersecurity knowledge and awareness among university employees.

5.2 Awareness of employees about cybersecurity

The data presented in Table 2 shows that 53.8% of respondents ranked their level of awareness as moderate, 15.4% as high, and 3.8% as very high. A low level of awareness was reported by 15.1% of respondents, while 11.3% of respondents ranked their awareness as extremely low. Interviews with management revealed the same. One manager had this to say: *"Since joining the university four years ago, I haven't received any formal training and am not even aware of the existence of an ICT policy."*

Table 2: Level of awareness about cybersecurity among employees

	Frequency	Percentage
Very Low	6	11.3
Low	8	15.1
Moderate	28	53.8
High	8	15.4
Very High	2	3.8
Total	45	100.0

Sources: Field data

According to this distribution, even though most employees have a moderate understanding of cybersecurity, there is still a considerable proportion of employees, more than a quarter, or 26.4%, who consider themselves to have a low to very poor awareness of the topic. In an academic setting, where personnel routinely handle sensitive digital material such as student records, research data, and administrative credentials, this is a cause for concern.

The fact that just 19.2% of respondents answered that they had a high or very high awareness of cybersecurity issues highlights the urgent need for education and training programs that are implemented across the entire institution on cybersecurity. The results of this study indicate that there is a gap between a fundamental acquaintance with cybersecurity dangers and practices and a profound, actionable comprehension of these topics.

The findings provide further evidence in support of the primary assumption of the research, which states that there are significant awareness gaps among university staff, which may leave the institution susceptible to cyber attackers. Furthermore, this data suggests that although the foundation of awareness may exist (as indicated by the high number of responses that were classified as moderate), it needs to be elevated through structured interventions to move more employees toward high or very high levels of awareness and engagement with cybersecurity best practices. This corroborates the theoretical framework of the study as well as Hadlington's (2017) findings, which emphasize that inadequate employee preparedness significantly increases an organization's vulnerability.

Table 3: Association between gender and awareness

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7.299[a]	4	**.121**
Likelihood Ratio	8.159	4	**.086**
Linear-by-Linear Association	.052	1	**.820**
No. of Valid Cases	52		

Table 3 shows the association between gender and cybersecurity awareness levels. Pearson Chi-Square p-value (0.121), Likelihood Ratio p-value (0.086), and Linear by Linear association p-value (0.820) are greater than the 0.05 level of significance, indicating that cybersecurity awareness and gender have no association.

Table 4: Chi-square test of age and level of cybersecurity awareness

Chi-Square test	**Value**	**df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	8.894[a]	12	.712
Likelihood Ratio	11.137	12	.517
Linear-by-Linear Association	.019	1	.891
N of Valid Cases	52		

Table 4 shows the association between age and cybersecurity awareness levels. All p-values, like Pearson's Chi-Square p-value (0.712), Likelihood Ratio p-value (0.517), and Linear by Linear association p-value (0.891), are greater than the 0.05 significance value, concluding that cybersecurity awareness and age have no significant association. Model Fit analysis is made to find the association between education level and cybersecurity awareness among employees

Table 5: Model Fitting of education level and awareness

Model Fitting Information				
Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	45.780			
Final	38.350	7.430	3	**.059**

The analysis above assesses the model fit between education level and awareness. The chi-square significance value is 0.059, which is just above the conventional 0.05 threshold. This suggests a potential trend or emerging relationship between education level and awareness.

Table 6: Goodness of fit in ordinal regression

	Chi-Square	df	Sig.
Pearson	10.591	9	.305
Deviance	12.522	9	.185

Table 6 tests the goodness of fit of awareness and education level. Both Pearson's (0.305) and Deviance significance (0.185) values are greater than the level of significance (0.05), showing that the model fits the data well. Thus, the model adequately confirms the association between education level and the level of awareness.

Table 7: Parameter estimates for education level and level of awareness

		Estimate	Std. Error	Wald	df	Sig.
Threshold	Very Low	-3.314	.706	22.063	1	.000
	Low	-2.203	.619	12.655	1	.000
	Moderate	.522	.506	1.061	1	**.303**
	High	2.408	.788	9.342	1	.002
Location	Certificate	-1.452	.767	3.582	1	**.058**
	Diploma/Advanced Diploma	-1.067	.810	1.735	1	.188
	Bachelor	-1.961	.769	6.508	1	.011
	Master's Degree and above	0[a]			0	

Source: Field data

The above table shows the parameter estimates for the Level of education and awareness. Among the threshold parameters, it is evident that very low, Low, and high are less than the level of significance of 0.05; thus, they are significant. Therefore, it says that the change in education level affects the changes in the level of awareness. Further in the location parameter, certificate qualification has a 0.058 significant value, indicating the potential trend that lower qualification has lower awareness.

Diploma and advanced diploma qualifications indicate a weak relationship between this level of education and awareness levels. Individuals with bachelor's and master's degrees are notably less likely to fall into higher awareness categories.

Objective 2: Identify and discuss common cybersecurity threats encountered by employees in their daily work environment.

Both online surveys and face-to-face interviews revealed that some personnel errors, whether intentional or inadvertent, contribute to cyberattacks. The organizational ICT infrastructure and deficiencies in security policies and procedures were identified as the source of cyber risks. The vulnerabilities categorized under several classifications are presented below.

5.2.1 Employees' vulnerabilities with safe browsing

Figure 1 illustrates varying degrees of safe browsing vulnerabilities among users. The most critical gap lies in the ability to detect suspicious emails, followed by unsafe sharing of personal information and unsafe downloading practices. These findings suggest that while some awareness exists, there are significant shortcomings in email threat recognition and data handling practices. Tailored cybersecurity education and training, particularly around phishing and safe email practices, would help mitigate these vulnerabilities and strengthen the institution's cybersecurity posture.

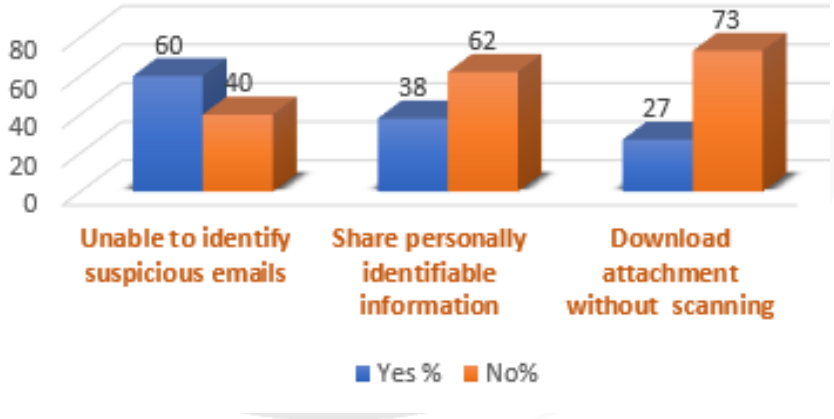

Figure 1: Vulnerability-safe browsing
Source: Field data

5.2.2 Employees' vulnerabilities with passwords

Table 4 demonstrates that 72% do not alter their passwords at regular intervals, 39% share passwords with colleagues, and 65% utilize the same password across multiple accounts. Face-to-face interview responses revealed that the university lacked stringent cybersecurity standards.

Table 4: Cumulative percentage of password vulnerabilities under different categories

Not changing passwords at regular intervals	72%
Share the password with their colleagues	39%
Using the same password for different accounts	65%

Source: Field data

The statistic indicating that 72% of respondents do not consistently update their passwords implies a pervasive disregard for fundamental cybersecurity practices. Frequent password updates are crucial to reduce the threats associated with compromised credentials. Neglecting to do so renders accounts increasingly vulnerable to illegal access, particularly if the passwords have been compromised or deduced.

With 39% acknowledging the exchange of passwords, there is a distinct breach of optimal data security protocols. Password sharing compromises accountability and traceability; when numerous individuals possess the same credentials, pinpointing the origin of any security violation becomes challenging. This action may also signify a deficiency in comprehension or awareness of the associated risks.

Individuals who utilize identical passwords across various accounts, including 65%, are particularly susceptible to credential stuffing attacks, wherein a compromise in one system may grant attackers access to further accounts (Itro, 2023; Jawaid, 2022). This reutilization exacerbates the potential harm of any singular breach, jeopardizing both personal and institutional data.

The in-person interviews indicated that the university does not possess rigorous cybersecurity standards, hence contextualizing the aforementioned facts. The lack of institutional policies or enforcement mechanisms undoubtedly adds to the lenient conduct of staff and students. In the absence of explicit standards, training, or enforcement, users are less inclined to adhere to security procedures. The results underscore a more extensive cultural problem, rather than mere individual carelessness.

Objective 3: Examine employees' attitudes and practices towards cybersecurity protocols and policies

5.2.3 Vulnerabilities associated with nonadherence to security practices

Table 5 highlights the following cybersecurity lapses: 71.2% of the respondents do not read security updates shared by the IT department, 52.3% fail to report cyber-related issues, 59.4% do not protect sensitive files with passwords, and 53.8% neglect safe disposal practices.

The data presented in Table 5 underscores significant gaps in cybersecurity awareness and compliance among the respondents. The most prevalent issue is the failure to read security updates from the IT department, with 71.2% admitting to this lapse. This suggests a general lack of engagement with crucial information that could help prevent cyber threats, possibly due to low digital literacy, information overload, or a perceived lack of relevance.

Furthermore, 52.3% of respondents do not report cyber-related incidents to IT, which can severely compromise the organization's ability to respond to threats promptly. This may stem from a lack of clear reporting protocols or fear of repercussions.

The fact that 59.4% do not protect sensitive files with passwords indicates poor data handling practices, increasing the risk of unauthorized access or data breaches. This could reflect inadequate training or a lack of emphasis on data security policies.

Lastly, 53.8% failing to follow safe disposal practices — such as shredding printed documents or wiping storage devices — highlights a critical vulnerability in the end-of-life management of sensitive information.

Collectively, these findings point to the urgent need for enhanced cybersecurity training, clearer policies, and a more proactive IT communication strategy to foster a culture of cyber responsibility within the organization.

Table 5: Cumulative percentage of vulnerabilities associated with nonadherence to security practices

Not reading the security updates shared by IT	71.2%
Not reporting cyber-related issues to IT	52.3%
Lack of protection for sensitive files with passwords	59.4%
Not adhering to safe disposal practices	53.8%

Source: Field data

6. Recommendations

- Awareness, training, and education programs need to be conducted at regular intervals to equip staff with adequate awareness and defend against threats.
- Policies and procedures should be reviewed frequently to meet the new demands and challenges by getting guidance from experts in the field.
- The university should have policies related to passwords, safe disposal practices, and the sharing of devices.
- Separate printers should be used for printing sensitive documents. viii) Files or documents shared by staff in the common folder need to be authorized by the team head to ensure that sensitive and confidential contents are not shared with all staff.

7. Implications for policy

The findings of the study highlight the urgent need for the review and enforcement of the ICT policy within the university. Such a policy should clearly articulate expected cybersecurity behaviors, outline procedures for reporting threats or breaches, and specify consequences for non-compliance. It must be effectively communicated to all staff and reviewed periodically to remain aligned with evolving cyber threats. Furthermore, the study indicates a lack of formal training among staff, which underscores the importance of instituting a policy that mandates regular cybersecurity training for all employees. This training should be a compulsory component of staff development programs to enhance overall institutional resilience.

In addition, institutional policies must include robust protocols on handling emails, attachments, and personally identifiable information. These protocols should be aligned with national and international data protection standards, and they should be accompanied by enforceable guidelines that promote accountability. Another key implication is the need to integrate cybersecurity responsibilities into human resource management practices. For instance, cybersecurity awareness and compliance should form part of job descriptions, onboarding programs, and performance assessments. Lastly, the university should implement a policy that supports regular monitoring, including cybersecurity audits and compliance checks. This would help track progress, identify emerging risks, and ensure staff adherence to cybersecurity standards.

8. Implications for practice

Practically, the university should initiate routine cybersecurity awareness campaigns aimed at reinforcing safe digital practices among employees. These campaigns may include posters, newsletters, email reminders, and brief workshops focused on topics such as phishing, password security, and safe browsing. Creating a culture of cybersecurity awareness requires continuous engagement and reinforcement. Moreover, there is a strong case for establishing a dedicated cybersecurity support team or help desk to provide real-time assistance to staff, respond to reported incidents, and offer ongoing guidance on best practices.

To enhance responsiveness, the university should implement a user-friendly reporting mechanism that allows staff to easily report suspicious activities or potential breaches. This system should be accessible and anonymous if needed, thereby encouraging more active participation in threat detection. Recognizing that cybersecurity risks vary by role, it is essential to provide differentiated training that is tailored to specific job functions.

Furthermore, incorporating practical exercises such as phishing simulations can significantly improve staff preparedness by providing hands-on experience in recognizing and reacting to threats. These simulations should be conducted regularly to assess real-time responses and reinforce learning. Finally, cybersecurity should be seamlessly integrated into daily work routines. Staff should be encouraged to adopt safe digital habits such as scanning email attachments before opening, using strong and unique passwords, and avoiding the sharing of sensitive information through unsecured channels. Collectively, these practices can help mitigate vulnerabilities and foster a more secure and informed working environment.

10. Conclusions

This case study examined cybersecurity awareness among employees in a private university in Papua New Guinea, revealing a moderate level of awareness overall. While a significant portion of employees demonstrate good understanding of cybersecurity practices, a concerning number remain highly vulnerable to cyber threats. This vulnerability includes risky practices such as password sharing, infrequent password changes, and a lack of adherence to secure data disposal procedures. Encouragingly, the study also highlighted the adoption of certain positive security habits, including proper shutdown routines and consistent use of screen locks. However, the lack of engagement with security updates, reluctance to report potential threats, and inadequate training opportunities represent significant areas requiring immediate attention.

To sustain a cybersecurity posture within these institutions, a multi-faceted approach is crucial. Prioritizing comprehensive training programs that address identified vulnerabilities and promoting best practices is paramount. Furthermore, fostering a culture of security consciousness through regular communication and awareness campaigns will empower employees to become active participants in safeguarding sensitive information. By addressing these critical areas, higher education institutions can take significant steps towards mitigating cyber risks and ensuring a secure digital environment.

This study is grounded in protection motivation theory; however, the findings contrast with the theory, as employees at the university exhibit reluctance to implement cybersecurity protocols, reflecting a disconnect between awareness and actual behavior.

References

Admass, W. S., Munaye, Y. Y., & Diro, A. A. 2023. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031

Akers, R. 2017. Social learning and social structure: A general theory of crime and deviance. *Routledge*. https://doi.org/10.4324/9781315129587

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L. 2017. Gender difference and employees cybersecurity behaviors. *Computers in Human Behavior*, 69: 437-443.

Azinheira, B., Antunes, M., Maximiano, M., & Gomes, R.P. 2023. Information security and cybersecurity assessment in SME – an implementation methodology. *Journal of Global Business and Technology*, 19(1): 78-95.

Chugh, J., & Taqa, A. 2019. Cyber-Physical System (CPS) & Internet of Things (IoT) in manufacturing. *International Journal of Applied Engineering Research*, 8(2).

CISA .2022. CISA cybersecurity awareness program. Available at: www.cisa.gov/cybersecurity-awareness-month [Accessed: 30 June 2024].

Cucinotta, D., & Vanelli, M. 2020. WHO declares COVID-19 a pandemic. *Acta Biomed*, 91(1):157–160.

Daengsi, T., Pornpongtechavanich, P & Wuttidittachotti, P. 2022. Cybersecurity awareness enhancement: a study of the effects of age and gender of thai employees associated with phishing attacks. *Educational Information Technology (Dordr)*, 27(4): 4729-4752. doi: 10.1007/s10639-021-10806-7.

Faroukhi, A.Z., El Alaoui, I., Gahi, Y., & Amine, A. 2020. Big data value chain: A unified approach for integrated data quality and security, *Journal of Big Data*, 7(1):1-17. Available at: https://doi.org/10.1186/s40537-019-0281-5

Fosoh, H.N. & Amaechi, A.O., 2022. *An assessment of employee knowledge, awareness, attitude towards organizational cybersecurity in Cameroon*. Network and Communication Technologies, 7(1): pp.1–11.

Hadlington, L. 2017. Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7). doi:10.1016/j.heliyon.2017.e00346.

Internet Crime Complaint Center (IC3).2023. Internet Crime Report. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf [Accessed 22 Apr. 2024].

Itro, D. 2023. 8 considerations when establishing cybersecurity in higher education. *EDUCAUSE.* Available at: https://er.educause.edu/articles/2023/8/8-considerations-when-establishing-cybersecurity-in-higher-education [Accessed: 24 June 2024].

Jawaid, S.A. 2022. Cyber security threats to educational institutes: A growing concern for the new era of cybersecurity. *International Journal of Data Science and Big Data Analytics*, 2(2).

Kamiya, S., Kang, J., Kim, J., Milidonis, A., & Stulz, R.M. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms, *Journal of Financial Economics*, 139(3): 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kaplan, A. M. 2015. Social media, the digital revolution, and the business of media. *International Journal on Media Management*, 17(4) :197–199. doi: 10.1080/14241277.2015.1120014.

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

Li, L., He, W., Xu, L., Ash, I., Anwar, M. & Yuan, X. 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45: 13-24.

MeitY. 2022. Cyber Swachhta ReevesKendra. Available at: www.csk.gov.in/index.html [Accessed: 7 May 2024].

NCSC.2022. The national cyber security centre. Available at: www.ncsc.gov.uk/ [Accessed: 4 April 2024].

Ntloedibe, T., Foko, T. & Segooa, M.A. 2024. Cloud leakage in higher education in South Africa: A case of University of Technology, *South African Journal of Information Management*, 26(1). a1783. https://doi.org/10.4102/sajim.v26i1.1783.

Radio New Zealand. 2021. PNG government system hit by ransomware attack, *Radio New Zealand*, 29 October. Available at: https://www.rnz.co.nz/international/pacific-news/454467/png-government-system-hit-by-ransomware-attack

Reeves, A., Delfabbro, P., & Calic, D. 2021. Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *Sage Open,* 11(1). https://doi.org/10.1177/21582440211000049.

Rogers, R. W. 1975. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology: Interdisciplinary and Applied*, 91(1): 93–114. https://doi.org/10.1080/00223980.1975.9915803

SANS Institute. 2023. SANS 2023 Security Awareness Report: Managing Human Risk. https://assets.contentstack.io/v3/assets/bltabe50a4554f8e97f/blteeccffa7b4d55709/SANS_SSA_Security-Awareness-Report_2023.pdf

Shah, P., & Agarwal, A. 2023. Cyber suraksha: a card game for smartphone security awareness, *Information and Computer Security*, 31(5): 576–600.

Shi, Z., Ritter, A., Mueller, G., & Wright, E. 2019. Analyzing the perceived severity of cybersecurity threats reported on social media. *Proceedings In the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies.* [online] Available at: https://doi.org/10.18653/v1/N19-1140 [Accessed 9 Jul. 2025].

Sonja, R. 2011. More technology use means increase in cyber threats: Case study: Innovation in cyber risk management. *Business Insurance*, 45(13).

Sophos .2022. Sophos threat report: Gravitational force of ransomware black hole pulls in other cyberthreats to create one massive, interconnected ransomware delivery system. Available at: https://www.sophos.com/en-us/labs/security-threat-report [Accessed: 8 June 2024].

Tazi, F., Shrestha, S. & Das, S. 2023. Cybersecurity, safety, & privacy concerns of student support structure for information and communication technologies in online education, *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2: 264): 1–40.

Tolossa, D.N. 2023**.** Importance of cybersecurity awareness training for employees in business. *Vidya - A Journal of Gujarat University*, 2(2): 104–107. https://doi.org/10.47413/vidya.v2i2.206

Wang, J., Li, Y., & Rao, H. R. 2017. Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research,* 28(2): 378–396. [online] Available at: https://doi.org/10.1287/isre.2016.0680 [Accessed 9 Jul. 2025].