International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I8P103

Volume 73 Issue 8, 28-41, August 2025

Original Article

Assessing Information Security Landscape Among End-Users Using PPT Framework

Noli B. Lucila Jr.

Information Technology Department, College of Science, Bicol University, Legazpi City, Philippines.

[1]*Corresponding Author : nlucila@bicol-u.edu.ph*

Received: 07 February 2025 Revised: 05 July 2025 Accepted: 21 July 2025 Published: 30 August 2025

Abstract - *Information security's importance in education has grown significantly in the digital age as educational institutions utilize technology to improve the learning experience. From the existing literature, although numerous studies have focused on security technologies, research on end-user factors has been scarce. Therefore, this study evaluates the information security landscape among end-users in an educational setting based on the People, Process and Technology (PPT) Framework. A Likert scale survey was given to 192 personnel and 378 students to obtain primary data through validated scales and items relating to research objectives based on the Center of Internet Security (CIS) Controls. The findings revealed the university's security strengths, weaknesses, and areas for improvement to enhance resilience against emerging threats. This study, like others, has limitations, such as not including the university's network infrastructure and security operations.*

Keywords - *Information security, Information security landscape, Security practices, PPT framework, People-process-technology.*

1. Introduction

The field of Information Technology (IT) is characterized by rapid and continuous advancement. In order to be competitive, firms must adapt to the rapidly evolving landscape of mobile devices, applications, the Internet, and social media. However, when new IT products are introduced, new weaknesses are identified and transformed into emerging threats, leading to the recognition of new security risks associated with them. In the current rapidly changing IT settings, numerous challenges have arisen in ensuring an efficient information security system to safeguard and manage crucial digital assets. Currently, the utilization of IT is the most crucial element in responding to security threats.

Nowadays, most organizations are highly concerned about information security (infosec). Consequently, organizations have allocated substantial financial resources towards implementing IT solutions [1, 2] to safeguard themselves against security risks. Organizations have been using technical measures like firewalls, Intrusion Protection Systems (IPS), and antivirus software to safeguard their company systems and networks. Some experts and scholars, however, contend that infosec should not solely prioritize technology solutions. Instead, it should also encompass the human dimension, particularly in terms of their behavior and involvement in security measures [3, 4]. Moreover, it is commonly recognized that the primary threats to the company's infosec are posed by individuals within the organization [5]. Although it is commonly believed that most digital threats originate from external sources, both external attackers and insiders are widely recognized as posing significant risks [6]. Additionally, recent surveys indicate that the primary cause of infosec breaches is human factors, specifically the improper or excessive use of computer resources [7], as well as deliberate or unintentional actions [8], and inexperienced or inadvertent human behaviors [9]. According to recent research on security breaches, it has been found that employees' incompetence or lack of knowledge leads to poor security measures, which in turn result in significant financial losses [10, 11]. Naive individuals exemplify the use of digital tools without awareness, inadvertently disclosing their usernames and passwords, or oversharing personal information on social media platforms [3, 12]. However, some have contended that while end-users are often seen as the most vulnerable aspect of infosec, they are also recognized as the most crucial asset in safeguarding organizations from diverse threats [13]. Consequently, they are referred to as "the first line of defense" [14]. The success of an organization's security activities is determined by the dedication and competence of end-users, as evidenced by studies conducted by [15-17]. Hence, it is imperative for organizations to incorporate the human element into a comprehensive security strategy. According to the research, insiders, specifically employees, and likely trusted computer and mobile devices, have emerged as a significant security concern [12, 18, 19]. The increasing prevalence of the

Internet, including social media and cloud services, along with the rising use of mobile devices, has made it increasingly challenging to implement effective information security measures. Indeed, some scholars and professionals contend that technical solutions that neglect the human element are increasingly becoming outdated. Hence, it is crucial for every end-user to actively implement robust security measures, particularly due to the widespread adoption of remote work and their frequent access and management of vital organizational assets and resources.

It is also crucial to prioritize education, awareness, and communication in enforcing infosec. These techniques are not only cost-efficient but also very effective in security management [3, 16]. Various studies indicate that security awareness and training can influence an end-user's security-related behavior, leading to the development of a security-conscious workforce [18, 20]. Furthermore, educational institutions are becoming rapidly digital, which makes them more vulnerable to cybersecurity threats. However, most of the research that has been done so far has focused on businesses or governments. There has been much less research on educational institutions, where different user roles and limited resources can make infosec management more difficult, especially in developing countries like the Philippines, which deal with end-user security awareness, process maturity, and technology adoption. Therefore, this study fills in the gaps by looking at the current state of information security at a Philippine higher education institution using the People, Process, and Technology (PPT) framework. This study is unique because it looks at the security knowledge of end users, institutional processes, and security technology use in an academic community as a whole. Moreover, the study gives useful, actionable information that can help with targeted awareness programs, process improvement, and technology investments in higher education settings by looking at these three areas in a systematic way. The results add to both theory and practice by showing that the People, Process, and Technology Framework [21] is useful in the education sector of a developing country and by suggesting ways to improve the institution's overall security posture.

Like previous scientific undertakings, this study has limitations. This research study excluded the current organizational network and security configuration, including enterprise network infrastructure, production servers, information systems, and other critical organizational assets. Publishing this information publicly could increase the danger of external and internal attacks, undermining the organization's security. Furthermore, in addition to its practical contributions supported by empirical data and outcomes, this research also makes a theoretical contribution to the expanding field of infosec research literature, particularly its utilization of the PPT Framework as a unique theory.

2. Review of Related Literature

In today's corporate landscape, the majority of firms have made infosec a key priority due to the growing number of security risks and threats. Infosec denotes the protection of information and information systems from illegal access, use, disclosure, disruption, alteration, or destruction. The objective is to ensure information confidentiality, integrity, and availability [22]. Over time, infosec has evolved into a socio-technical problem as it encompasses not just technology, but also human elements [3, 23, 24]. Infosec encompasses users' perception of the importance of security, their responsibilities, practices, and their appropriate level of security for the enterprise. Because cyber threats are getting more advanced, information security has become a major issue for all businesses. Previous studies indicate that human error and lack of awareness are still two of the most common reasons for security incidents. Furthermore, there has been a lot of research on security awareness and technology use in both the public and private sectors, but not much on how to fully integrate people, processes, and technology in higher education settings, especially in developing countries.

This shows a gap in research: limited real-world evidence on how colleges and universities can create comprehensive, balanced, and long-lasting information security programs that include user awareness, strong processes, and up-to-date technology. This study helps fill that gap using the PPT (People, Process, Technology) framework in higher education. It provides real-world data that can help shape policy and practice in schools that are dealing with changing cyber threats.

2.1. People, Process and Technology Framework

The People, Process, and Technology (PPT) framework was based on Harold Leavitt's model from the 1960s. Leavitt's original diamond model has four parts: people, technology, structure, and tasks. These parts need to work together to improve the performance of the organization. After that, the parts of the structure and tasks were combined into a single "process", which led to the creation of the well-known PPT Framework. In recent decades, the PPT Framework has been utilized in several research projects to facilitate organizational changes and transformations [25], enhance service quality [26], and drive process innovations [27].

Based on the literature discussion, the term "People" refers to the human resources responsible for carrying out the work, also known as "process workers". "Process", on the other hand, includes the specific steps and actions that need to be taken, how a group of people should be organized, and how people and technology should work together to reach certain goals. Finally, "technology" means the tools and methods people use to do things more quickly and easily. Figure 1 shows a Venn diagram of the PPT framework, which is a common way to show the balance between the three pillars. Another way to show it is as a golden triangle.

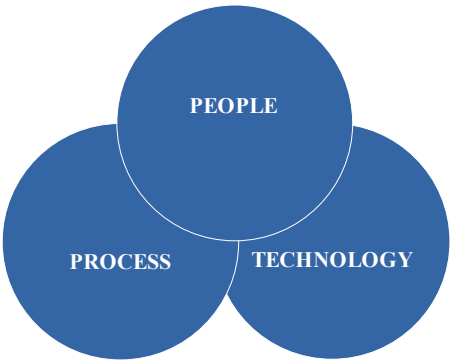

Fig. 1 People, process, technology framework

[21] introduced the application of the PPT framework in the field of infosec during the late 1990s when he established his internet security company. However, according to certain sources, the Information Technology Infrastructure Library (ITIL), a framework of best practices for delivering information technology services established in the 1980s, also utilized PPT as a fundamental idea [28]. Furthermore, numerous studies have employed the PPT Framework in the realm of infosec research. [18] analyzed the ramifications of zero trust, a security framework for building and executing IT systems, on individuals, procedures, and technology. Similarly, [29] argued that incorporating security into software development should involve considering PPT factors. In addition, [30] introduced an integrated Network Operation Center (NOC) and Security Operation Center (SOC) that identified PPT as the fundamental components. Additionally, the PPT framework was employed to assess the security maturity level based on NIST guidelines. Moreover, previous research has demonstrated that neglecting to assess the significance of people, process, and technology can jeopardize the effectiveness of introducing and executing system improvements [31]. Similarly, within the realm of infosec, businesses must examine PPT aspects in order to adopt a comprehensive security approach [30, 32].

2.2. People Aspect

Multiple sources affirm that human resources are essential assets in an organization [33, 34]. However, within the domain of infosec, individuals are commonly perceived as the most vulnerable aspect [35, 36]. This can be attributed to the lack of knowledge and carelessness of end-users [37]and the deliberate and accidental misuse and exploitation of resources [38]. Moreover, they are the preferred focus of external attackers [39] owing to their limited understanding of potential vulnerabilities to cyberattacks and other critical security concerns prevalent in the majority of organizations [40]. Despite being viewed as a potential weakness, humans are recognized as the primary asset in protecting valuable and crucial information and resources. Therefore, numerous authors have regarded human resources as the primary means of protection [41]. According to [2], the most efficient means of enhancing security defense is to augment awareness and preparedness through education and training. It is imperative for organizations to focus on the human elements by cultivating an informed and proactive workforce [42]. Many businesses have adopted a comprehensive strategy by recognizing the significance of human factors in safeguarding their vital resources.

Moreover, existing literature has demonstrated that employees' awareness of infosec plays a crucial role in reducing risks and effectively handling infosec breaches [43]. Measuring employees' awareness is crucial for safeguarding a business from cyber threats. This practice has gained significance in both corporate and individual/private settings in recent times [44]. Therefore, it is crucial for all employees to possess knowledge of the policies and processes that regulate the safeguarding of sensitive information within their organization. Furthermore, as stated by [45], infosec awareness encompasses two key elements: (1) the extent to which employees understand infosec behavior, and (2) the degree of dedication and adherence to the recommended practices specified in infosec policies, regulations, and guidelines.

A separate study conducted by [46] examines the perspectives of insiders regarding their participation in infosec activities. It also compares these perspectives with those of infosec professionals and gathers comments from insiders regarding the effectiveness of recommended measures to address infosec challenges. In addition, [5] conducted a comprehensive study that adopts a holistic perspective, considering individual, organizational, and technical aspects. The investigation focused on examining these elements to demonstrate the potential impact of human factors vulnerabilities on cybersecurity threats. Additionally, it evaluated healthcare organizations' development level by employing qualitative and quantitative research techniques to determine their ability to respond to and protect against cyberattacks. The study argues that a higher level of cyber security culture does not always mean that people will follow the rules and laws more. Also, adding non-technical preventive measures, like making users more aware, along with traditional technical solutions, can create a complete and unified plan for managing cybersecurity in businesses.

2.3. Process Aspect

Risk management is crucial for ensuring the security of information, as it helps protect organizational assets such as information systems and network resources from potential threats that could compromise the confidentiality, integrity, and availability of information [40]. In essence, risk can be described as the likelihood that a specific danger will take advantage of weaknesses in an asset or collection of assets, resulting in harm or loss to the asset [47]. In essence, a security risk refers to the possibility of an undesirable event taking place as a result of the presence of a threat and the exposure of vulnerabilities in assets [48, 49]. In general, a security threat

can originate from either natural or man-made sources, as well as from an individual or a collective entity. These threats have the capacity to cause significant damage or disruption to an organization's information, operations, and other valuable assets [50]. Similarly, security threats refer to the presence of enemies who have the ability to carry out actions that could potentially undermine the organization's interests [51]. Evaluating and examining risks are the two main elements of risk management. Risk assessment involves the identification, characterization, and analysis of risks. Moreover, it is crucial to assess threats based on their severity and identify the specific regions that require protection [40].

However, there is a prevalent argument that ordinary users may possess insufficient understanding regarding certain security threats [46]. Therefore, users must actively engage in security risk management, acknowledge the security threats, and implement appropriate security measures to ensure awareness of information security [52]. Furthermore, multiple sources have contended that all assets are vulnerable to a range of risks, some of which may go unnoticed by the asset owners [49]. Therefore, users must know about the system's weaknesses, potential sources of harm, and the specific events that could take advantage of these vulnerabilities. Additionally, it is crucial to identify and apply the most efficient security measures that offer the most value for money [22].

2.4. Technology Aspect

Existing literature suggests that infosec practitioners and researchers primarily rely on technological solutions to prevent security breaches [53]. The technological aspects of infosec encompass software, hardware, and processes. Implementing infosec controls is crucial for safeguarding an organization's information assets, reputation, integrity, personnel, and other resources [22]. However, numerous studies argue that achieving the highest level of security in an organization requires considering governance, security management, and security controls as well [32]. Therefore, it is also essential for insiders or ordinary users to align with the goals of infosec specialists and understand the necessary security precautions. [54] In theory, an ideal security measure should be both non-intrusive to individuals' rights and simultaneously ensure safety, reliability, and efficacy. On the same note, several research studies in the literature have examined and appraised various security systems within a business.

The study conducted by [55] examines the variables and criteria that are important for evaluating security technologies. It also provides recommendations for effective security measures and technologies that do not violate privacy and are socially acceptable. Additionally, it assessed the legitimacy of the trade-off between security and privacy by studying the viewpoints of both the scientific community and citizens regarding the connection between surveillance, privacy, and security. Moreover, [56] contend that herd behavior impacts users' security decisions, contrary to the viewpoint of other researchers who propose that individuals make logical choices regarding security technologies based on their understanding of security threats. In addition, the research demonstrated that the inclination to imitate others as a result of the herd behavior phenomenon, wherein individuals disregard their own understanding and imitate others when faced with uncertainty about a security technology, has a more significant influence on security decisions than the perceived effectiveness of the technology.

3. Materials and Methods

Surveys were the main way to collect data, and the main material was a well-designed survey questionnaire based on the Center of Internet Security (CIS) Controls. These controls are basic security practices that are meant to keep things clean and safe from cyberattacks. The survey used closed-ended and open-ended questions to collect numbers and words about the state of infosec.

The survey was about security awareness, security controls, security tools and technology, and security practices and processes, including managing risks and breaches. The informed consent papers presented to the participants made it obvious what the study was about, made it plain that they were free to take part, and stated that their data would be kept private. Using informed consent ensured that the study was done in a way that was morally right.

3.1. Sources of Data

Students, faculty, and non-teaching staff at Bicol University in Legazpi City, Philippines, both technical and non-technical, participated in the survey. A convenience, non-probability sampling technique was used to choose the respondents.

3.2. Data Analysis

The quantitative approach included examining survey results using descriptive statistical data. The survey received responses from 378 students, 192 teachers, and other staff members. A systematic sampling method was used to make sure that students from different colleges and departments were included. The goal of this plan was to get a range of viewpoints on the state of information security. Surveys were distributed via Facebook chat, Google Forms, email, and other platforms. The researcher conducted a quantitative analysis of closed-ended responses using statistical software such as Microsoft Excel. Lastly, the data was carefully examined to ensure its consistency and completeness, ensuring its quality.

3.3. Ethical Issues

During the whole process of gathering data, the principle of informed consent was scrupulously followed. Also, any information that was collected was kept completely private because it was about security. So, the results and findings of

this study project were kept secret so that no information about the participants, including their names and work titles, could be linked to them.

4. Results and Discussion

This section presents the research study's empirical results, which give a full picture of the infosec landscape within the examined setting. The survey included 570 faculty, non-teaching staff and students from a higher education institution in the Philippines. The results were examined through the lens of people, process, and technology.

4.1. People

Because cyber threats are becoming more common and complicated, infosec is important for both people and businesses. The results show that the end-users who were surveyed have a good understanding of basic infosec concepts. Participants had a very good understanding of password security, which is often thought to be the main way to keep people from getting into their accounts illegally. To protect personal and business data from cyberattacks, it is important to know all the password security measures, such as using strong and unique passwords, not sharing passwords, and turning on two-factor authentication. Participants' knowledge of information security was rated on a scale of 1 to 5 in six key areas: security policies, password security, phishing awareness, data handling, device security, and social engineering. The average score was 3.85 out of 5. Table 1 shows the average scores for these areas. The average score for password security (4.27) and phishing (3.84) shows that participants were very aware of these topics. However, the participants were not as aware of data handling (3.74) and social engineering (3.53). Recent studies have shown that the best ways to protect their account are to keep their passwords clean and be able to avoid phishing attacks. Similarly, participants showed how to use secure passwords by using strong, unique credentials, not sharing passwords, and turning on multi-factor authentication. This shows that the institution's efforts to raise awareness about security are effective.

However, there are still a lot of things the end-users do not know about, such as how to prevent social engineering, keep devices safe, and handle data. In addition, participants did not know much about how to safely delete data or encrypt it. Also, the participants knew little about social engineering techniques like pretexting, baiting, and tailgating, which means they need more specific training. Previous studies have shown that social engineering is still one of the most common ways to attack because it relies on people making mistakes. In short, the institution has a good culture of cybersecurity awareness, but to stay safe from new threats, people need to learn more about advanced infosec practices through ongoing, personalized education. Cyber threats are becoming more common and complicated, so it is important for both people and businesses to protect their data. The results show that the participants know a lot about basic infosec concepts. This is a good sign that participants are learning how important it is to keep their personal information safe is. Also, the end-users who took part in the study knew a lot about how to keep their passwords safe, which is often thought to be the best way to keep people from getting into their accounts without permission.

In a cross-tabulated format, Table 2 shows the average scores for each age group on information security awareness. This makes it easy to determine the difference between the scores of different groups of people. Young adults (ages 18 to 29) were always more aware in all areas, with an average score of 4.05. Senior adults (ages 60 and up) had an average score of 3.42. Young Adults scored 4.45 on password security, and Senior Adults only scored 3.80; Young Adults averaged 3.80 on social engineering awareness, and Senior Adults only averaged 3.00. These results suggest that younger people spend more time online and are more likely to know about new cybersecurity threats and best practices. On the other hand, older people may not be as familiar with new attack methods like social engineering and may rely more on old or traditional security habits. These differences show how important it is to make appropriate awareness programs for different ages and meet the unique learning needs of older workers. These programs should focus on modern social engineering techniques, password hygiene, and how to handle data. The overall pattern shows that there is a need to take a different approach to security education so that all user groups in the institution are ready to recognize and deal with modern cyber threats. The results also show that the end-users who were studied were very aware of phishing. Phishing is a common problem in today's digital world. It involves tricking people into giving up private information like login details or financial data. To lower the risk of data breaches and financial loss, end-users need to be able to spot and protect themselves from phishing attacks. The fact that end-users are now more aware of phishing shows that efforts to educate them on how to spot phishing emails and websites have been somewhat successful.

Table 1. Mean awareness scores across key information security domains

Awareness Domain		Mean
Security Policies Awareness		
	Aware of the organization's information security policies and procedures	3.54
	Aware of the organization's acceptable use policy for technology and information resources	3.56
	Aware of the consequences of violating information security policies in your workplace	3.82
	Aware of the potential risks associated with not following security policies	3.89

	Aware of the specific security measures in place for protecting sensitive information	3.71
		3.70
Password Security Awareness		
	Aware of the consequences of not changing your password regularly	4.21
	Aware of using strong, unique passwords for different accounts	4.51
	Aware of using unique passwords for each of your accounts, including work and personal accounts	4.47
	Aware of the risks associated with using the same password across multiple platforms or accounts	4.30
	Aware of the organization's policies regarding password sharing and accountability	3.85
		4.27
Phishing Awareness		
	Aware of the common signs of a phishing email (e.g., suspicious links, email addresses)	3.97
	Aware of the potential risks and consequences of falling victim to phishing attacks	4.15
	Aware of the common lures used in phishing emails (e.g., urgent requests, financial incentives, fake invoices)	4.03
	Aware of the security features in modern email systems that help detect phishing attempts	3.54
	Aware of the security features in web browsers that help detect phishing websites	3.52
		3.84
Data Handling Awareness		
	Aware of the potential risks and consequences of mishandling sensitive data	4.13
	Aware of the classification of data in your organization (e.g., public, confidential, sensitive)	3.84
	Aware of the proper procedures for storing sensitive data securely	3.69
	Aware of the process for data backup and recovery in case of data loss or system failure	3.65
	Aware of the encryption methods used to protect sensitive data within your organization	3.37
		3.74
Device Security Awareness		
	Aware of the potential risks and consequences of using insecure devices in your role	3.90
	Aware of the common threats to device security, such as malware or unauthorized access	3.95
	Aware of the risks associated with sharing login credentials	4.12
	Aware of the importance of using strong and unique passwords for your devices	4.39
	Aware of the measures in place for securing personal devices that connect to company networks	3.71
		4.01
Social Engineering Awareness		
	Aware of the term "social engineering" in the context of cybersecurity	3.08
	Aware of the common social engineering tactics (e.g., impersonation, pretexting)	3.22
	Aware of the potential risks and consequences of falling victim to social engineering attacks	3.28
	Aware of the potential risks of sharing personal or sensitive information with unknown individuals or entities	4.04
	Aware of the risks associated with clicking on links or downloading attachments from unknown or suspicious sources	4.02
		3.53
	OVERALL MEAN	**3.85**

Table 2. Mean information security awareness scores across age groups (n=570) for key domains

Awareness Domain	Young Adult (18–29)	Adult (30–39)	Middle Age (40–59)	Senior Adult (60+)	Overall Mean
Security Policies	3.85	3.72	3.54	3.40	3.70
Password Security	4.45	4.35	4.10	3.80	4.27
Phishing Awareness	4.05	3.95	3.70	3.50	3.84
Data Handling	3.95	3.85	3.60	3.30	3.74
Device Security	4.20	4.10	3.80	3.50	4.01
Social Engineering	3.80	3.60	3.30	3.00	3.53
Overall Mean	**3.92**	**3.93**	**3.67**	**3.13**	**3.85**

There are a few more areas where infosec awareness could be improved. For instance, the participants know phishing and password security but do not know much about social engineering, device security, or safe data handling. Further, to stop sensitive information from being revealed or accessed by unauthorized parties, it is essential to comprehend and put into practice secure data management strategies like encryption, data minimization, and secure destruction. By raising awareness of device security measures like installing software updates, configuring antivirus software, and enforcing strict access restrictions, the risk of malware infections and unauthorized access to devices can be decreased.

In addition, since hackers commonly use social engineering to fool people into disclosing personal information or taking actions that jeopardize security, it is imperative to address problems with people's comprehension of the technique. Teaching end-users about common social engineering tactics like baiting, tailgating, and pretexting may help them identify and steer clear of these dishonest practices. Generally, the level of information security awareness among participants is encouraging, but further study and instruction are needed to improve preparedness for new cyberthreats. By promoting a culture of ongoing learning and awareness, individuals and organizations can strengthen their ability to protect themselves against information security threats in a world that is becoming more digitalized and networked.

4.2. Process

Security practices involve several operations associated with the Identify, Protect, Detect, Respond, and Recover functions, all of which help enhance the organization's cybersecurity stance. There is potential for enhancing the uniform application of security approaches and processes within the organization. Table 3 compares how personnel and students handle information security across the five NIST Cybersecurity Framework functions: Identify, Protect, Detect, Respond, and Recover. Overall, students had higher mean scores (3.32) than the personnel (2.72), which suggests that students were more familiar with and followed recommended infosec practices. Students were more careful about keeping track of their software and active accounts (mean = 3.30) than the personnel (mean = 2.58), which shows that they were more organized about being aware of their assets. In the Respond function, students also had a higher average score of 3.64 compared to 3.24 for personnel. This shows they took more proactive steps to fix unauthorized software or manage inactive accounts. The Protect function had a big difference between personnel and students: personnel averaged only 2.81, while students averaged 3.29. This gap shows that both groups say they use anti-malware, firewalls, and password controls moderately, but personnel are less consistent in using more advanced security measures like encrypting data at rest and in transit, managing patches, and turning off auto-run features. The Detect function was the weakest for both groups, with average scores of 2.32 for staff and 3.11 for students. The respondents in particular did not use automated software inventory tools, behavior-based anti-malware, or host-based intrusion detection, which shows that they are very vulnerable to not being able to find threats quickly. Neither group was ready to keep, isolate, and test backups regarding the Recover function. Personnel were again behind students (mean 2.66 vs. 3.29). This suggests that while students seem to be in a moderate recovery posture, personnel may be more likely to experience extended downtime or data loss after a security incident because their recovery plans are not complete or have not been thoroughly tested. Overall, these results show that students have a pretty good understanding of infosec in all five areas. However, the staff is behind, especially when it comes to advanced detection and recovery strategies. This pattern shows that targeted awareness campaigns, technical skills training, and automated controls should be at the top of the list of things to do to close these important gaps, especially for the personnel group. The fact that students do better in all areas all the time suggests that being familiar with technology may be a protective factor that should be built on. At the same time, making institutional policies stronger and getting more support from leaders can help both groups grow when it comes to information security.

The average score of 3.02 out of 5.0 for assessing and evaluating infosec practices for end-users suggests a modest level of efficacy. This average score indicates that there are strengths and weaknesses in the university's overall infosec stance. The moderate score suggests that the university is currently adopting infosec measures, but there is room for improvement to make these measures more effective. These areas may encompass user training, incident response, network monitoring, and other crucial parts of a holistic security plan. Thus, it is crucial to integrate and coordinate multiple security measures.

Table 3. Mean information security practice scores across the NIST cybersecurity framework functions, comparing personnel and students

INFORMATION SECURITY PRACTICES	Personnel	Students
IDENTIFY		
Establish and maintain an inventory of installed software on your computer	2.48	3.22
Maintain a list of active accounts on your computer	3.04	3.68
Use an automated vulnerability scanner to check the vulnerabilities of your computer	2.21	2.98
	2.58	**3.30**
RESPOND		
Take necessary action when you find unauthorized software installed on your computer	3.54	4.03

Practice automatic device lockout on your portable devices, such as laptops and cell phone devices	3.28	3.61
Disable dormant (unused) accounts, such as Guest or other default accounts, on your computer	2.89	3.26
	3.24	**3.64**
PROTECT		
Practice encrypting your sensitive or important data in your removable media , such as flash drives, external hard drives	2.12	3.05
Practice encrypting sensitive or important data in transit, such as sending it via email	2.09	2.93
Practice encrypting data at rest, particularly your sensitive or important data stored in your hard drives	2.00	2.97
Use or enable automatic session locking on your computer device (i.e. it automatically locks after a period of inactivity)	3.22	3.37
Use a firewall on your computer	3.24	3.37
Proactively manage default and/or other active accounts, such as Guest, on your computer	2.57	3.05
Check unnecessary services running on your computer, and uninstall and disable them when needed	3.09	3.57
Use a unique password for every account	3.88	3.93
Enable the automated operating system (e.g. Windows) patch management	2.89	3.31
Enable the automated application (e.g. MS Office, web browsers) patch management	2.85	3.45
Use an anti-malware software (e.g. antivirus) to protect your system from spreading or executing malicious applications, code or scripts such as viruses, worms	3.40	3.69
Enable your antivirus to automatically update for anti-malware signatures	3.36	3.53
Disable the auto-run and auto-play features for removable media (e.g. inserting flash drives into your USB	3.00	3.26
Do you enable the anti-exploitation features of your anti-malware software (e.g. antivirus)	2.46	3.11
Protect your recovery (backup) data	3.17	3.66
Use a host-based intrusion prevention solution on your computer	2.17	2.84
Use an application-layer firewall on your computer	2.22	2.87
	2.81	**3.29**
DETECT		
Use an automated software inventory tool to detect the software installed on your computer	2.05	3.12
Configure your anti-malware application (e.g. antivirus app) to automatically scan your removable media for viruses and other malicious software	2.82	3.39
Use behavior-based anti-malware software (your antivirus can detect and protect your system from malware such as ransomware, zero-day malware, and lifeless malware)	2.33	3.06
Use a host-based intrusion detection solution on your computer	2.06	2.87
	2.32	**3.11**
RECOVER		
Perform automated backups for your system	2.82	3.35
Maintain an isolated instance of your recovery (backup) data	2.68	3.29
Test or check your recovery (backup) data	2.47	3.23
	2.66	**3.29**
Overall Mean	**2.72**	**3.32**

Figure 2 shows the average information security practices of the personnel and students in the five NIST cybersecurity functions. The chart shows that the Detect and Recover functions have big gaps, especially among staff, who only scored an average of 2.32 in Detect compared to 3.11 for students. In the same way, the average score for the personnel on the Recover functions was 2.66, while the average score for students was 3.29. These scores show that automated software inventory, host-based intrusion detection, and systematic backup validation procedures are not being used as much as they should be.

All of these are important for spotting threats early and getting systems back up and running after an event. On the other hand, both groups did well in the Respond function (3.24 for staff and 3.64 for students), which shows that the participants were comfortable with tasks like disabling unused accounts and setting up automatic device lockouts. But even in Respond, the personnel are still a little behind the students. The radar diagram makes it very clear that the Detect and Recover functions need the most urgent attention, especially for the personnel who consistently scored lower in all five areas.

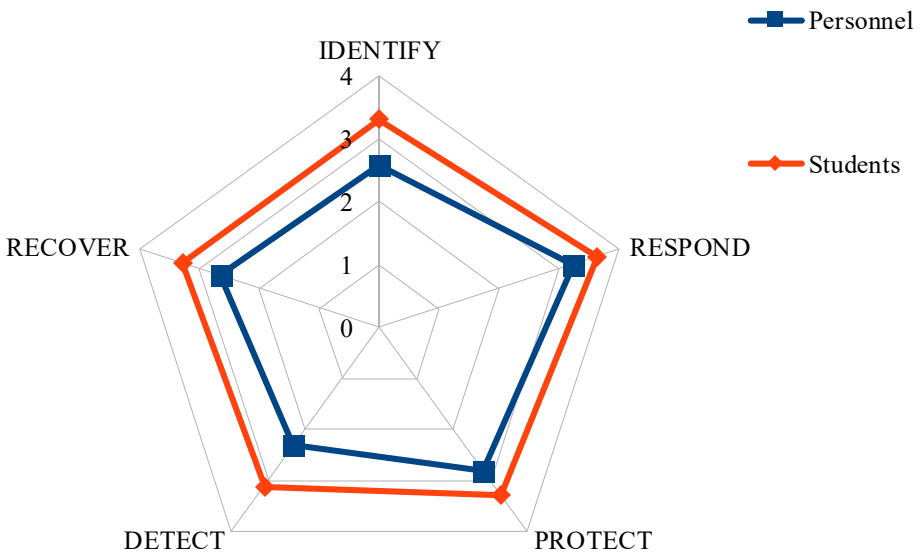

Fig. 2 Radar diagram of the average scores of information security practices for personnel and students across the five NIST cybersecurity functions

This supports putting awareness campaigns and technical controls at the top of the list to improve detection and recovery readiness. These things fill in gaps that could leave the institution open to long-term cyberattacks or incomplete data restoration. Also, for infosec practices to work, end-users need support from leaders. Making users more aware and educated, especially about how to spot social engineering threats and how to handle data safely, will help make the security environment stronger. Furthermore, the results show how important it is to combine technical strategies with human elements. It is important to use security technologies, but it is also important to train users well. Also, teaching end-users about important security protocols in a focused way can help improve cybersecurity. In general, the average scores for security procedures show how safe the university community is.

4.3. Technology

The infosec technology adoption survey results showed that participants were willing to pay for security tools to keep their important and private data safe. In the fast-paced world of cybersecurity, end-users are using the latest hardware and software to strengthen their digital defences. The more the digital world grows, the more dangerous it becomes. Because of this, it is more important than ever to have strong security measures in place. This has led to the development of many different security solutions. End-users are using a lot of different technologies to protect their work and personal digital spaces, such as antivirus software, firewalls, and multi-factor authentication. Cloud-based services and mobile devices have also made keeping all parts of the organization's digital ecosystem safe harder. For example, many end-users use Windows Firewall and other firewalls, which have a big share of the market. Firewalls are important for keeping a network safe because they stop people from getting in without permission. Many of the respondents also use Identity and Access Management (IAM) systems, such as biometrics and password management. IAM is important for following the principle of least privilege, which means that it controls who can access systems and data. However, fewer respondents use encryption tools like BitLocker, FileVault, or DiskCryptor. Encryption methods are very important for keeping private and sensitive information safe. Also, fewer respondents used IPS/IDS technologies like Snort. Even though the usage is low, these technologies are very important for keeping an eye on how networks and systems work to find and stop security incidents. Moreover, fewer people use VPNs, which are very important for keeping communications safe and private, especially when working from home. Table 4 shows that antivirus software (79%) and firewalls (62%), which are traditional perimeter-based security controls, were the only ones that were widely used. Only 27% of people used identity and access management tools. This means that there are some ways to check a user's identity, but they are not fully developed yet. It is noted that fewer end-users used advanced security tools like encryption (15%), virtual private networks (8%), intrusion prevention/detection systems (8%), and vulnerability scanners (2%). This pattern shows that layered defense strategies, which are needed to protect against new and more sophisticated cyber threats, have big holes in them. Furthermore, the results show that it needs a better defense-in-depth strategy that makes better use of these technologies.

Table 4. Bar chart showing adoption rates of security technologies among respondents (n=570), highlighting high usage of traditional tools but lower uptake of advanced security controls

Technology Tool	Usage Rate (%)
Antivirus (e.g. McAfee, Avast, Microsoft Defender)	79%
Firewall (e.g. Windows Firewall, ZoneAlarm)	62%
Identity and Access Management (e.g. passwords, biometrics, and keycards)	27%
Encryption Tools (e.g. BitLocker, FileVault, DiskCryptor)	15%
Virtual Private Networks (e.g. OpenVPN)	8%
Intrusion Prevention/Detection (e.g. Snort)	8%
Vulnerability Scanners (e.g. Tripwire, Nmap, OpenVAS)	2%

In the same way, the average scores for the information security rules in Table 5 show how well the institution is using them. The average score for Account Management was 3.80. This suggests that end-users are doing an excellent job of remembering their passwords, turning off accounts they do not use, and keeping track of their credentials. Malware Defenses (3.58) and Email and Web Browser Protections (3.55) also achieved strong rankings, which implies that there are defenses against prevalent online threats.

Some parts, on the other hand, were very weak. For example, Network Monitoring and Defense (mean = 2.24) was the least useful of all the controls. This means that no tools, such as intrusion detection or prevention systems, can help end-users find dangers before they happen. Audit Log Management (mean = 2.49) and Security Awareness and Skills Training (mean = 2.59) were also two of the lowest-ranking areas. This illustrates that there are issues with both keeping an eye on things and end-users wanting to be safe.

The average score of 2.62 for data protection methods also demonstrates that not everyone used encryption or other safe ways to handle data all the time. Incident Response Management (3.04) and Continuous Vulnerability Management (2.96) both obtained average scores. This suggests that checking for vulnerabilities and being ready to deal with incidents could be better. This viewpoint, which is based on rank order, suggests that most of the time, standard security methods, notably those that protect accounts and malware, work well. However, it will take a lot of work to make things like network monitoring, audit logs, and structured security awareness programs stronger. These statistics show that these sectors that are not doing as well should focus on specific investments and training initiatives. This will assist in keeping the data safe and sound.

The people, process, and technology framework used for the infosec evaluation highlights how security flaws are connected and how vital it is to look at the whole system when trying to minimize risks. To keep outside dangers at bay, it is necessary for end-users to be aware of security issues and for processes to be strong. Training and raising awareness among end-users is vital to make security a part of the culture and minimize the chance of human error causing breaches.

The university also needs to make sure that security is continually improving. This includes regular audits, training for how to handle problems, and risk assessments that look ahead to make sure they can handle emerging risks. Finally, it is necessary to put money into updating and improving the security technology infrastructure so that it can manage new problems and stay strong in a world where threats are becoming more complex. The university may improve its overall security and minimize its risks by looking at the evaluation results in each area of the people, process, and technology framework.

Table 5. Mean ratings of information security control practices among respondents, ranked by perceived implementation effectiveness

Information Security Control	Mean
Account Management	
Observe a good practice in managing your accounts, such as maintaining an inventory of accounts, using unique passwords and disabling dormant accounts	**3.80**
Malware Defenses	
Actively run anti-malware software (e.g. antivirus) on your computer to prevent or control the installation, spread, and execution of malicious applications, code, or scripts	**3.58**
Email and Web Browser Protections	
Enable your security tools (e.g. anti-spam software, anti-adware, pop-up blockers) in your browser to actively improve the protection and detection of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement	**3.55**
Data Recovery	
Perform data recovery (backup) practices sufficient to restore the pre-incident and trusted state	**3.40**
Secure Configuration of Enterprise Assets and Software	

Establish and maintain security configuration in your computer, such as automatic session locking (i.e. automatically locks after a period of inactivity), automatic device lockout, disable default accounts and unnecessary services	**3.39**
Access Control Management	
Observe a good practice in granting, managing and revoking rights and privileges for other user accounts for digital resources (i.e. file sharing, printer sharing)	**3.35**
Incident Response Management	
Properly respond (e.g. handle, manage and report) to security incidents	**3.04**
Inventory and Control of Software Assets	
Actively manage (make an inventory, track and correct) installed software on your computer device	**3.00**
Continuous Vulnerability Management	
Assess and track vulnerabilities in your computer in order to remediate and minimize, the window of opportunity for attackers	**2.96**
Data Protection	
Use data protection controls such as encryption tools to identify, classify, securely handle, retain, and dispose of data	**2.62**
Security Awareness and Skills Training	
Recognize social engineering attacks, and be able to practice proper data handling techniques	**2.59**
Audit Log Management	
Enable the audit logging feature available in your operating system (e.g. Windows) to collect audit log events that could help you detect, understand, or recover from an attack	**2.49**
Networking, Monitoring and Defense	
Install user-based/host-based tools (e.g. host-based Intrusion Protection System – IPS; host-based Intrusion Detection System – IDS) to establish and maintain network monitoring and defense against security threats	**2.24**
Overall Mean	**3.08**

5. Conclusion

In conclusion, this evaluation of the university's information security, which examined people, procedures, and technology, helped us better understand our current situation. It demonstrated what is effective, what is not, and where changes are required. By adopting a comprehensive approach, the study identified the critical elements that influence our security and offered workable solutions to bolster our defenses against ever-evolving cyberthreats. The university ought to think about investing in more contemporary security equipment in the future, such as upgraded encryption systems and potent antivirus software. To further safeguard our systems, it would also be prudent to implement cutting-edge techniques like identity and access management, behavior analytics, and threat intelligence. By taking these actions, we can strengthen our security posture and be ready to respond to emerging threats. All things considered, this study serves as a guide for enhancing our security and lowering risks.

The university can safeguard its assets, uphold public confidence, and strengthen its standing as a safe and dependable establishment in the modern digital world by heeding its advice. The results also demonstrated that although some of our current security procedures are effective, others must be strengthened in order to meet emerging threats. To ensure that our security measures actually function as intended, user awareness and training are particularly crucial. Additionally, maintaining a strong security foundation requires staying up to date with emerging technologies. Investing in cutting-edge tools will help us stay ahead of increasingly complex cyberattacks. Ensuring that our security measures adhere to industry standards and regulations is another top priority, as it helps safeguard our data and reputation. Lastly, in order to identify vulnerabilities before they can be exploited, the university should plan frequent security audits. By being proactive, we can keep our systems safe and deal with issues early.

5.1. Limitations of the Research

This study primarily focused on end-users, specifically examining the infosec methods in use. Similar to other research, this study also has several limitations. This research study did not include the current organizational structure of network and security operations, as this is classified and cannot be shared with the general public due to the potential risk of external and internal attacks. Disclosing this information could endanger the security of the university's network infrastructure and other critical systems. Although this study offers vital insights into infosec measures in the investigated setting, it is crucial to recognize specific constraints that could affect the application and extent of the findings. The results of this study may not be generally applicable to other organizational environments because they rely on the specific context. The unique characteristics, organizational culture, and technology infrastructure of the context under study can influence the effectiveness of

information security protocols differently than in other contexts. Cybersecurity is always changing because of new threats and improvements in technology. The information security measures that were looked at in this study accurately show the state of cybersecurity in the area that was looked at at a certain point in time. The findings may not be as important if technology changes quickly, organizations change their structures, or new threats appear. The study's data also came from answers that end users gave themselves. Even though people try to give accurate and honest answers, they may still be affected by response bias or social desirability. It is possible that the answers given by participants were influenced by their own biases and did not honestly reflect what they did or thought.

Last but not least, the study mostly looked at certain infosec protocols, which are important but only a small part of the bigger picture when it comes to cybersecurity. If these are the only indicators that are brought up, other important things that affect the university's overall security may be missed.

5.2. Future Research Direction

Future research should try to get around these problems by doing cross-industry studies, using a wider range of infosec protocols, using a longitudinal research framework, and checking how well measures work against new cybersecurity threats. Also, doing a comparison analysis in different types of organizations could help us better understand the things that affect how well information security works.

References

[1] Alexandra Borgeaud, IT Security Services Spending Worldwide 2017-2024, Statista, 2025. [Online]. Available: https://www.statista.com/statistics/217362/worldwide-it-security-spending/

[2] Thomas J. Parenty, and Jack J. Domet, *A Leader's Guide to Cybersecurity: Why Boards Need to Lead--and How to Do It*, Harvard Business Review Press, Boston, MA, USA, 2019. [Google Scholar] [Publisher Link]

[3] William J. Triplett, "Addressing Human Factors in Cybersecurity Leadership," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 573-586, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Isabella Corradini, *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap between People and Digital Technology*, 1st ed., Springer, Cham, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Alessandro Pollini et al., "Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach," *Cognition, Technology & Work*, vol. 24, no. 2, pp. 371-390, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Andreea Bendovschi, "Cyber-Attacks - Trends, Patterns and Security Countermeasures," *Procedia Economics and Finance*, vol. 28, pp. 24-31, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[7] Khando Khando et al., "Enhancing Employees Information Security Awareness in Private and Public Organizations: A Systematic Literature Review," *Computers & Security*, vol. 106, pp. 1-22, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Neeshe Khan, Robert J. Houghton, and Sarah Sharples, "Understanding Factors that Influence Unintentional Insider Threat: A Framework to Counteract Unintentional Risks," *Cognition, Technology & Work*, vol. 24, no. 3, pp. 393-421, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Kathryn Marie Parsons et al., "The Influence of Organizational Information Security Culture on Cybersecurity Decision Making," *Journal of Cognitive Engineering and Decision Making*, vol. 9, no. 2, pp. 117-129, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[10] Kamy Farahbod, Conrad Shayo, and Jay Varzandeh, "Cybersecurity Indices and Cybercrime Annual Loss and Economic Impacts," *Journal of Business and Behavioral Sciences*, vol. 32, no. 1, pp. 63-71, 2020. [Google Scholar]

[11] Md. Haris Uddin Sharif, and Mehmood Ali Mohammed, "A Literature Review of Financial Losses Statistics for Cyber Security and Future Trend," *World Journal of Advanced Research and Reviews*, vol. 15, no. 1, pp. 138-156, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Jason E. Thomas, "Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks," *International Journal of Business Management*, vol. 13, no. 6, pp. 1-24, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[13] Uchenna Daniel Ani, Hongmei He, and Ashutosh Tiwari, "Human Factor Security: Evaluating the Cybersecurity Capacity of the Industrial Workforce," *Journal of Systems and Information Technology*, vol. 21, no. 1, pp. 2-35, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] "*The New Users' Guide: How to Raise Information Security Awareness*," General Report, The European Union Agency for Cybersecurity, 2010. [Google Scholar] [Publisher Link]

[15] Rodrigo Hickmann Klein, and Edimara Mezzomo Luciano, "What Influences Information Security Behavior? A Study with Brazilian Users," *JISTEM-Journal of Information Systems and Technology Management*, vol. 13, no. 3, pp. 479-496, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[16] Abdul Rahman Ahlan, Muharman Lubis, and Arif Ridho Lubis, "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures," *Procedia Computer Science*, vol. 72, pp. 361-373, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[17] Clay Posey et al., "Motivating the Insider to Protect Organizational Information Assets: Evidence from Protection Motivation Theory and Rival Explanations," *The Dewald Roode Workshop in Information Systems Security 2011*, Blacksburg, Virginia, USA, pp. 1-51, 2011. [Google Scholar] [Publisher Link]

[18] Matthew Bush, and Atefeh Mashatan, "From Zero to One Hundred: Demystifying Zero Trust and its Implications on Enterprise People,

Process, and Technology," *Queue*, vol. 20, no. 4, pp. 80-106, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[19] Michael D. Richardson et al., "Planning for Cyber Security in Schools: The Human Factor," *Educational Planning*, vol. 27, no. 2, pp. 23-39, 2020. [Google Scholar] [Publisher Link]
[20] Ramakrishna Ayyagari, and Norilyz Figueroa, "Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets," *Journal of Information Systems Education*, vol. 28, no. 2, pp. 115-122, 2017. [Google Scholar] [Publisher Link]
[21] Bruce Schneier, People, Process, and Technology, Schneier on Security, 2013. [Online]. Available: https://www.schneier.com/blog/archives/2013/01/people_process.html
[22] Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri, *An Introduction to Information Security*, National Institute of Standards and Technology Special Publication, vol. 800, no. 12, pp. 1-101, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[23] Jongkil Jeong et al., "Towards an Improved Understanding of Human Factors in Cybersecurity," *IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, Los Angeles, CA, USA, pp. 338-345, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[24] Henry W. Glaspie and Waldemar Karwowski, "Human Factors in Information Security Culture: A Literature Review," *International Conference on Applied Human Factors and Ergonomics*, Los Angeles, California, USA, pp. 269-280, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[25] Uje D. Apeji, and Funlade T. Sunmola, "Principles and Factors Influencing Visibility in Sustainable Supply Chains," *Procedia Computer Science*, vol. 200, pp. 1516-1527, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[26] Bryan O'Nomerp O. Payawal, "*Integrative Action Research Paper on Improving the Service Quality of an Information Technology Service Team to Ensure Customer Retention*," Master's Thesis, De La Salle University, Manila, 2020. [Google Scholar] [Publisher Link]
[27] Joklan Imelda Camelia Goni, and Amy Van Looy, "Process Innovation Capability in Less-Structured Business Processes: A Systematic Literature Review," *Business Process Management Journal*, vol. 28, no. 3, pp. 557-584, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[28] Mircea Prodan, Adriana Prodan, and Anca Alecandra Purcarea, "Three New Dimensions to People, Process, Technology Improvement Model," *New Contributions in Information Systems and Technologies*, Springer, Cham, vol. 1, pp. 481-490, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[29] Valentina Tortoriello, "*Definition of a DevSecOps Operating Model for Software Development in a Large Enterprise*," Master's Thesis, Polytechnic University of Turin, pp. 1-129, 2022. [Google Scholar] [Publisher Link]
[30] Deepesh Shahjee, and Nilesh Ware, "Integrated Network and Security Operation Center: A Systematic Analysis," *IEEE Access*, vol. 10, pp. 27881-27898, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[31] Funlade T. Sunmola, and Alireza Javahernia, "Manufacturing Process Innovation Deployment Readiness from an Extended People, Process, and Technology Framework Viewpoint," *Procedia Manufacturing*, vol. 55, pp. 409-416, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[32] Milan Stojkov et al., "Towards Cross-Standard Compliance Readiness: Security Requirements Model for Smart Grid," *Energies*, vol. 14, no. 21, pp. 1-29, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[33] Hyun-Ju Choi et al., "Communities of Practice and Knowledge Management Systems: Effects on Knowledge Management Activities and Innovation Performance," *Knowledge Management Research & Practice*, vol. 18, no. 1, pp. 53-68, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[34] Retno Dwiyanti, Suwarti Suwarti, and Tri Naimah, "The Role of Organizational Culture Factors to Psychological Contracts (Transnational Contracts, Balance Contracts, and Relational Contracts)," *Journal of Advanced Research in Law and Economics (JARLE)*, vol. 9, no. 8(38), pp. 2570-2577, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[35] Steven Furnell, and Nathan Clarke, "Power to the People? The Evolving Recognition of Human Aspects of Security," *Computers & Security*, vol. 31, no. 8, pp. 983-988, 2012. [CrossRef] [Google Scholar] [Publisher Link]
[36] Zheng Yan et al., "Finding the Weakest Links in the Weakest Link: How Well do Undergraduate Students make Cybersecurity Judgment?," *Computers in Human Behavior*, vol. 84, pp. 375-382, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[37] Sorana Campean, "The Human Factor at the Center of a Cyber Security Culture," *International Journal of Information Security and Cybercrime (IJISC)*, vol. 8, no. 1, pp. 51-58, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[38] Nader Sohrabi Safa, "The Information Security Landscape in the Supply Chain," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 16-20, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[39] Nina Klimburg-Witjes, and Alexander Wentland, "Hacking Humans? Social Engineering and the Construction of the 'Deficient User' in Cybersecurity Discourses," *Science, Technology, & Human Values*, vol. 46, no. 6, pp. 1316-1339, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[40] Yvette Kamariza, "*Implementation of Information Security Policies in Public Organizations: Top Management as a Success Factor*," Master's Dissertation, Jonköping University (Jonkoping International Business School, JIBS, Informatics), 2017. [Google Scholar]
[41] Lena Y. Connolly, and David S. Wall, "The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomizing Countermeasures," *Computers & Security*, vol. 87, pp. 1-8, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[42] Emile Walker et al., Cybersecurity -The Human Factor: Prioritizing People Solutions to Improve the Cyber Resiliency of the Federal Workforce, Federal Information Systems Security Educators's Association, FISSEA, pp. 1-12, 2017. [Online]. Available: https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf

[43] Nader Sohrabi Safa, Rossouw Von Solms, and Steven Furnell, "Information Security Policy Compliance Model in Organizations," *Computers & Security*, vol. 56, pp. 70-82, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[44] Lennart Jaeger, "Information Security Awareness: Literature Review and Integrative Framework," *Proceedings of the 51st Hawaii International Conference on System Sciences*, Hilton Waikoloa Village, Hawaii, pp. 4703-4712, 2018. [Google Scholar] [Publisher Link]

[45] Kathryn Parsons et al., "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies," *Computers & Security*, vol. 66, pp. 40-51, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[46] Clay Posey et al., "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders," *Information & Management*, vol. 51, no. 5, pp. 551-567, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[47] Nancy A. Renfroe, and Joseph L. Smith, "*Threat/Vulnerability Assessments and Risk Analysis*," Applied Research Associates, Inc., pp. 1-9, 2010. [Google Scholar]

[48] Bako Ali, and Ali Ismail Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors*, vol. 18, no. 3, pp. 1-17, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[49] Halima Ibrahim Kure, Shareeful Islam, and Mohammad Abdur Razzaque, "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System," *Applied Sciences*, vol. 8, no. 6, pp. 1-29, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[50] Abhilash Panda, and Andrew Bower, "Cyber Security and the Disaster Resilience Framework," *International Journal of Disaster Resilience in the Built Environment*, vol. 11, no. 4, pp. 507-518, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[51] Christopher A. Ford, "International Security in Cyberspace: New Models for Reducing Risk," *Arms Control and International Security Papers*, vol. 1, no. 20, pp. 1-8, 2020. [Google Scholar]

[52] Ying Li, and Mikko Siponen, "A Call for Research on Home Users' Information Security Behaviour," *Pacific Asia Conference on Information Systems (PACIS) 2011 Proceedings*, vol. 112, pp. 1-11, 2011. [Google Scholar] [Publisher Link]

[53] Robert E. Crossler et al., "Future Directions for Behavioral Information Security Research," *Computers & Security*, vol. 32, pp. 90-101, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[54] Leon Hempel et al., "*Validated CRISP Methodology*," CRISP Project, pp. 1-91, 2015. [Google Scholar]

[55] Vincenzo Pavone, Sara Degli-Esposti, and Elvira Santiago Gómez, "*Key Factors Affecting Acceptance and Acceptability of Surveillance-Oriented Security Technologies*," SurPRISE Project European Union Framework 7 Security Research Programme, pp. 1-187, 2015. [Google Scholar]

[56] Ali Vedadi, Merrill Warkentin, and Alan Dennis, "Herd Behavior in Information Security Decision-Making," *Information & Management*, vol. 58, no. 8, 2021. [CrossRef] [Google Scholar] [Publisher Link]