Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 7
Open Access

Extent of Implementation and Level of Awareness of Employees on the Data Privacy and Cybersecurity Acts of Cagayan State University

Dorothy M. Ayuyang[1] and Richard R. Ayuyang[2]
College of Information and Computing Sciences, Cagayan State University, Gonzaga, Cagayan, Philippines
[1]dorothyayuyang@csu.edu.ph and [2]richard.ayuyang@csu.edu.ph

Cite this paper as: Dorothy M. Ayuyang ,Richard R. Ayuyang (2024). Extent of Implementation and Level of Awareness of Employees on the Data Privacy and Cybersecurity Acts of Cagayan State University. *Frontiers in Health Informatics*, *13 (7) 1074-1086*

Abstract
This research study aimed to investigate the extent of implementation and the level of awareness among employees concerning Data Privacy and Cybersecurity Acts within Higher Education Institutions (HEI) settings. The study explores the demographic profiles and online activities and engagement of the employees. An assessment was conducted to ascertain the current status of the implementation of Data Privacy and Cybersecurity Acts within the organization. This sought to evaluate how effectively these acts are enforced. The study also assesses the employees' level of awareness regarding Data Privacy and Cybersecurity Acts. This measurement aimed to evaluate their knowledge, understanding, and familiarity with the Data Privacy Act and the Cybercrime Prevention Act framework, which are relevant to the activities in higher education institutions. To determine whether variations in awareness exist among employees, the study groups individuals according to their profile variables. This analysis helps determine if certain groups differ in their awareness of data privacy and cybersecurity acts. To examine whether greater employee awareness leads to improved implementation, a correlation was executed between the status of data privacy and cybersecurity acts' implementation within the organization and the employees' level of awareness. The research study employed a descriptive-correlational approach, including surveys, and data analysis, which provided valuable insights into the extent of implementation and awareness among employees regarding Data Privacy and Cybersecurity Acts. Results show that there is a strong positive correlation between the level of awareness among employees and the implementation of data privacy and cybersecurity acts within the organization. The findings of this study will serve as a foundation for enhancing data protection and cybersecurity measures within the HEI setting and offer practical suggestions for improving the organization's overall cybersecurity system.

Keywords – *Data Privacy, Cybersecurity Awareness, Cybercrime, Data Protection*

I. INTRODUCTION

The recent pandemic had shocked the world because we are caught unprepared. Majority of institutions, school's government and private offices shifted to blended learning mode of delivery and a work-from-home mode which enabled the digital workspace and operations to continue online [1]. This has heightened the use of Information Communication Technology (ICT) devices, the web and the Internet. Consequently, the global ease of access to the internet has completely altered people's way of life. All these advancements have improved people's quality of life, but they have also led to an increase in crimes related to technology[2], particularly at the cyberspace which is known as the cybercrime. Malicious actors have taken advantage of the pandemic's abrupt changes in the digital landscape, particularly through the use of cyberattacks. Cyberattacks were noted as a security concern in developing nations like the Philippines as they may cause the paralysis of communication, infrastructure, international banking systems, crucial governmental functions, and defense/military command and control systems[3]. A report from an Interpol, found out that 907,000 spam messages, 737 incidents related to malware, and 48,000 malicious URLs that are related to the COVID-19 pandemic were detected[4]. Recently, news on cybersecurity breaches in private and government websites are

increasing which alerted the government to institutionalize more preventive measures to prevent data breaches (news.abs-cbn.com,2023).

Today's digital age, where internet technology and mobile applications has heightened its used and rapid advancement in all fields including Higher Education institutions, data privacy and cybersecurity have become paramount concern of all. Transformation on the way to digital interactions and data sharing become more inherent in our daily lives which led to the need to safeguard our personal and confidential information. Due to an increased reliance on technology, users are now the subject to this ever-increasing privacy threats [5]. Several studies on cybersecurity show that awareness to the organization's information security policy and procedures affects how competent employees are to manage their cybersecurity tasks[6], thus, reducing their risk to cyberattacks.

However, the extent of implementation and level of awareness among employees within HEIs regarding data privacy and cybersecurity measures vary significantly. Some employees are still unconvinced that their organization is vulnerable to cybercrime, and this aligns with the general public's lack of understanding or failure to address data security [7]. This variance gives both challenges and opportunities to these institutions to navigate the complex landscape of safeguarding data while simultaneously educating and engaging their workforce to foster culture of data protection.

Thus, the purpose of this study is to investigate the state of data privacy and cybersecurity knowledge and practices in HEIs, with a focus on evaluating the status of implementation and employee awareness. It also seeks to identify potential strategies for enhancing data protection and promoting a greater sense of responsibility among HEI employees. Specifically, it aims to (1) examine the demographic profile and online activities of the employees; (2) assess the status of implementation of data privacy and cybersecurity acts; (3) assess the level of awareness of the employees to data privacy and cybersecurity; (4) determine the potential differences in awareness based on demographic variables; (5) investigate the relationship between the status of implementation and level of awareness; and (5) identify key areas for recommendations based on the evaluation of results that could contribute to the development of a university cybersecurity system.

A. ***Conceptual Framework***

Figure 1 shows the conceptual model of the study which includes the variables to be considered in the study. This model provides a structured approach to assessing the state of data privacy and cybersecurity knowledge and practices which focuses on the implementation and awareness of employees within the context of HEIs. It integrates demographic analysis, assessment of awareness levels, and evaluation of implementation status.

The framework includes the demographic profile and online activities which provides context for analyzing data privacy and cybersecurity practices; level of awareness of employees to data privacy and cybersecurity which assess their knowledge of relevant laws, regulations and best practices; implementation of data privacy and cybersecurity which evaluates existing policies, procedures and infrastructure related to data protection and cybersecurity measures within the organization. The model used also examines the potential differences in awareness levels based on the demographic variables, the implementation status and the level of awareness of data privacy and cybersecurity measures which examines whether a higher level of implementation is associated with greater awareness among employees.

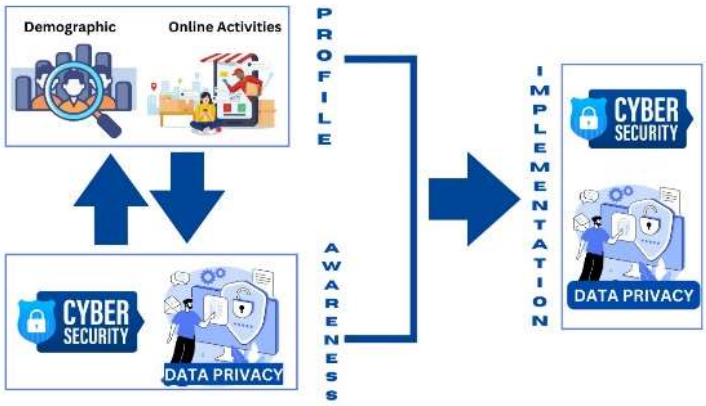

Fig. 1. Conceptual Model

B. ***Related Studies***

Personal Data Protection and Data Privacy of Employees

To protect personal information, many countries have begun enforcing the Data Privacy Act [8] to protect individual personal information in information and communications systems in the government and the private sector. Although the terms "data protection" and "data privacy" are frequently used interchangeably, there is a significant difference between the two. Data privacy defines who has access to data, whereas data protection provides tools and policies to limit data access. Compliance regulations help ensure that companies comply with user privacy requests, and companies are responsible for taking measures to protect private user data (cloudian,2022). Due to the risk of privacy violations and misuse of personal information, individuals consider personal data protection to be their top priority when engaging in online activities. This is why a right to data protection was introduced [9].

As modern organizations deal with an increasing amount of data and strategic information systems, the need to safeguard these critical assets becomes critical [10]. Because the purpose of communication and interaction is to process various types of information about individuals when they use a service or product, it is important to be clear how data is processed and protected [11]. As the march toward digital identity is well underway, the emphasis should be on both the adoption and adaptation of new structures and regulations. These are required to govern the related services and transactions, as well as to enact laws that impose penalties for violations [12].

Awareness of Security Policies for data protection

The continued incorporation of technology into daily life exposes technology users to increasing security and privacy risks [5]. However, employees are still skeptical about their company's vulnerability to cybercrime, according to Clutch's Grayson Kemper. While this is extremely frustrating for employers, employees' attitudes on the subject are consistent with the general public's ignorance or failure to address data security [7]. Maintaining the confidentiality, integrity, and availability of an organization's sensitive information system assets against attacks and threats is a challenge [13] and an employee information security awareness has become one of the critical aspects of protection against undesirable information security behaviors.

According to recent studies, employees who are aware of their company's information security policy and procedures are more competent to manage cybersecurity tasks than those who are not aware of their companies' cybersecurity policies [6]. However, as organizations need to increase their employees' security awareness and their capabilities to engage in safe cybersecurity behaviors, studies show that one factor that affect cybersecurity beliefs and behaviors of employees is associated with their gender differences which results that gender has some effect in the security self-efficacy, prior experience, and computer skills [14] of employees.

Compliance with organizations information security policies

To ensure compliance, some organizations have implemented their own information security policy to safeguard client's data. According to some research, many employees are either unaware of the policy or choose

to ignore it, which increases the risk of noncompliance. To assist organizations in managing compliance among their employees, a study was devised that used demographic factors to develop profiles of employees' policy awareness and intent to comply in order to educate employees accordingly, and it was discovered that these have significant effects on information security policy awareness and compliance [15]. However, some studies revealed that little attention was given to the concept of cybersecurity awareness within the networked industrial context, which are characterized by the use of advanced IoT (Internet of Things) technologies, big data analytics and cloud computing [16] which are now presently being the set-up in organizations.

As Higher education institutions (HEIs) become increasingly computerized to deal with large amounts of academic and operational data, there is a high risk of malicious exposure to internal and external threats. Despite the fact that the academic sector is making strides in the implementation of technical security controls, studies show that behavioral influence remains a challenge in the information security domain and findings confirms the significant contribution of institutional governance in motivating protection behavior among employees of HEIs [17].

II. METHODS

A. Research Design

This study used a quantitative research design utilizing descriptive correlational approach to examine the relationship between employees' awareness and implementation to data privacy and cybersecurity. Descriptively, the study ventures on the profiling of the respondents in terms of their demographic profile and their online activities.

B. Locale of the Study

This study was conducted in the nine (9) campuses of Cagayan State University Specifically, the study focused on the faculty members and administrative personnel who are regular in status of the university.

C. Respondents and Sampling Technique

The respondents of the study of 279 employees was selected using a simple random sampling technique. These samples which composed of 44 administrative personnel and 235 faculty members were drawn out of the total population of 1009 regular employees of the university. In selecting the sample size, a five percent (5%) margin of error was employed with fifty percent (50%) as the response distribution ensuring a representative sample of the university's employee demographic.

D. Data Collection Instruments and Procedures

As the study used a quantitative research design, numerical data were collected through primary sources in the form of a questionnaire as a data gathering tool which was administered through both online and printed formats to ensure maximum participation. The questionnaire consisted of three parts: Part 1 collected demographic information and details about online activities; Part 2 assessed the implementation status of data privacy and cybersecurity acts using a five-point Likert scale; Part 3 evaluated respondents' awareness of the Cybercrime Prevention Act and Data Privacy Act also using a five-point Likert Scale.

E. Analysis of Data/Statistical Treatment

This study used frequencies, percentages, ranks, weighted means and standard deviations in describing the profile of the respondents. To analyze the association among the relationships of variables, correlation analysis techniques were used which includes Bivariate Pearson Correlation, Spearman Rank/Rho, Point-Biserial Correlation whichever is appropriate for its associated variables. All inferential questions were tested at 0.05 level of significance.

To analyze the extent of implementation and level of awareness of the respondents, the 5-point Likert scale was use with its descriptive equivalent as shown in Table I for the Extent of Implementation and Table II for the Level of Awareness.

Table I: Extent of Implementation

Scale	Statistical Limits	Descriptive Value

		Extent of Implementation	***Description***
5	4.20 – 5.00	Very Evident	Strictly observe and implement the policy
4	3.40 – 4.19	Evident	Moderately observe and implement the policy
3	2.60 – 3.39	Somewhat Evident	Sometimes observe and implement the policy
2	1.80 – 2.59	Slightly Evident	Hardly observe and implement the policy
1	1.00 – 1.79	Not Evident	Never observe and implement the policy

Table II: Level of Awareness

Scale	**Statistical Limits**	**Descriptive Value**	
		Extent of Implementation	***Description***
5	4.20 – 5.00	Fully Aware	Possesses proficiency and knowledge on the issue
4	3.40 – 4.19	Aware	Can adequately understand the issue
3	2.60 – 3.39	Somewhat Aware	Can understand some aspects of the issue
2	1.80 – 2.59	Slightly Aware	Can understand the issue only with the guidance of the experts
1	1.00 – 1.79	Not Aware	Can hardly understands the issue even with the guidance from the expert

III. RESULTS AND DISCUSSIONS

A. *Demographic Profile*

For the result of distribution of the demographic profile, most of the employees are female with 59.1%, 71.3% married, 59.1% with master's degree, 64.9% without designation and 48.7% are instructors in position as shown in Fig. 2.

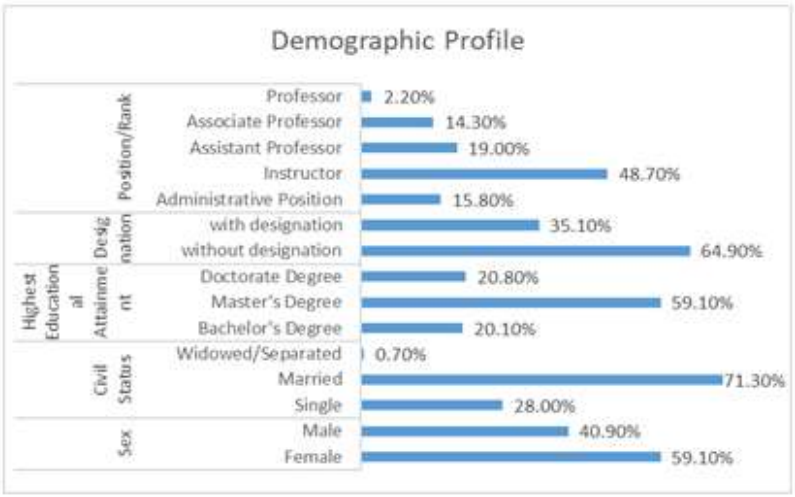

Fig. 2. Demographic Profile of the Employees

For the percentage distribution as to age, most of the respondents are at the age bracket of 30-36 as shown in Fig. 3. Also for the percentage distribution of the employees as to their years in service (Fig. 4.), most of them are in the service for

1-9 years.

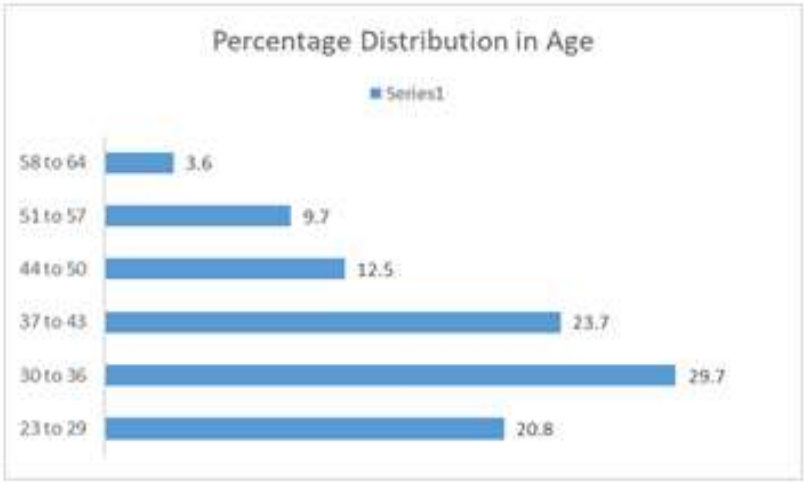

Fig. 3. Percentage Distribution in Age

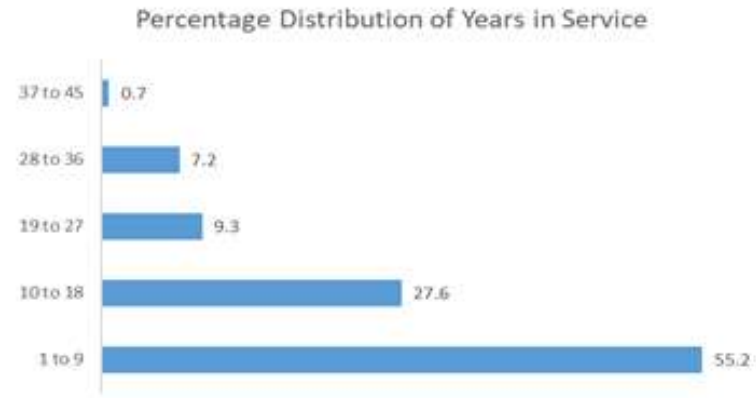

Fig. 4. Percentage Distribution of Years in Service

These demographic details provide a picture of the diverse backgrounds of the employees, which is an important factor in understanding the different levels of cybersecurity awareness and its implementation. Further, these statistics give insights into the digital engagement of the employees which is essential for designing the cybersecurity awareness initiatives within the university.

B. ***Online Activities***

For the percentage distribution of the respondents as to their online activities, as shown in Fig. 5 most of them have a digital skill level of intermediate with 59.1%, have laptop as their devices used with 35%. Most of them connects to a cellular data with 36.2% and mostly their purpose of using the internet is for social networks with 22.9%.

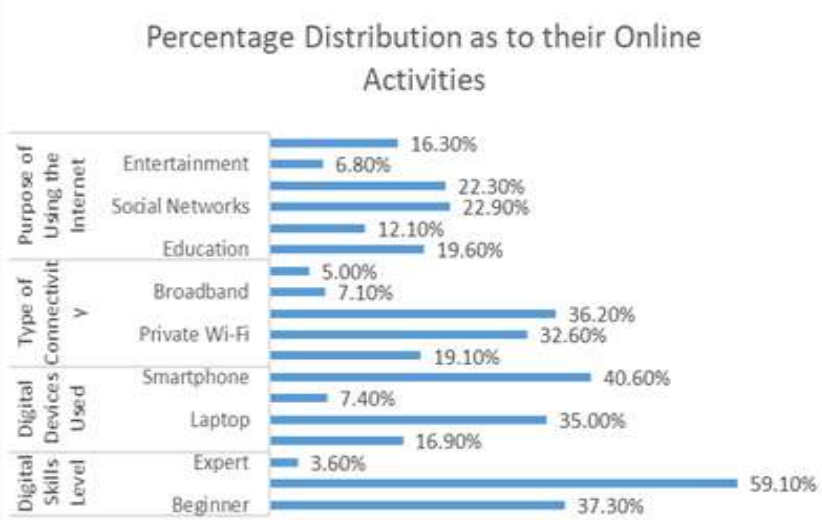

Fig 5. Percentage Distribution of Online Activities

In their daily usage of the internet, most of them is connected to the internet for an average of 1 to 5 hours per day as shown in Fig. 6.

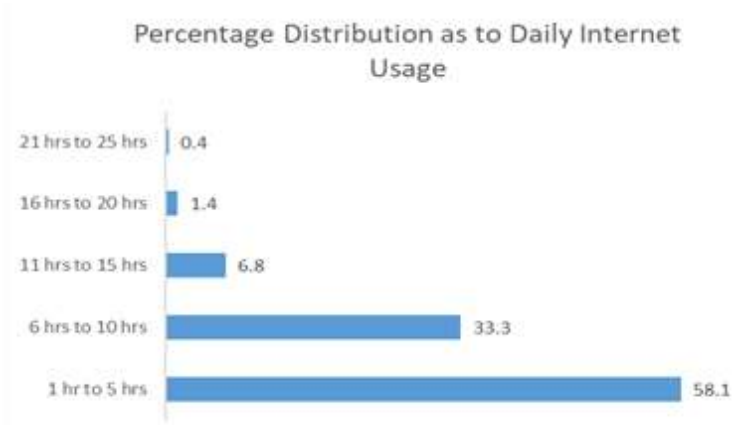

Fig. 6. Percentage Distribution as to Daily Internet Usage

The results provide useful information about the population's online activities which can help the organization and policymakers modify their digital programs and services to better meet the needs and preferences of the employees, thereby enhancing digital inclusion and accessibility. Furthermore, identifying areas where digital skills can be improved will help to design targeted training and education initiatives that will empower people to use digital technology more effectively.

Related papers also provide insights into the demographic profile of the employees and their online activities. In the study of [18], online employee profiles can provide information about the organization, its structure, and the elements that characterize their employees' social reach.[19], investigates the impact of demographic factors on organizational performance in the IT sector and concludes that several demographic variables influence performance. Also, from the study of [20], investigates the relationship between employees' demographic profile and perceptions of corporate culture, revealing variances based on gender, age, education level, and job experience in the IT sector.

These findings demonstrate that employees' demographic profile can influence their online activity and their awareness to cybersecurity.

*C. **Status of Implementation of Data Privacy and Cybersecurity***

Table III: Status of Implementation of Data Privacy and Cybersecurity

Statements	Mean	Descriptive Value
1. Data Privacy	4.02	Evident
2. Cybersecurity	4.07	Evident
Overall Weighted Mean	**4.04**	**Evident**

Table III shows the status of implementation of data privacy and cybersecurity in the university. For Data Privacy which include questions on the policies as to the protection of personal information of employee data and how it is being collected, processed and retained, result show that the policies are evidently implemented with a mean of 4.02. This means that the employees has a low knowledge of implementation when compared to the overall weighted mean of 4.04. However, for their Cybersecurity awareness which include questions on the access, use, and management of university data, devices and networks, the mean obtained was 4.07 which describes that the employees have a high knowledge of its implementation as compared to the overall weighted mean of 4.04. This reflects that the university's adherence to data privacy and cybersecurity standards and the effective implementation of relevant policies were moderately observed and implemented.

Key findings shows that the university has adequately and moderately established a policy that adheres to the principles of transparency, legitimate purpose, and proportionality as to the collection, processing, and retention of employee data. This demonstrates a commitment to safeguarding the privacy of employee information and ensuring that data handling practices align with legal and ethical standards.

On the acceptable use policy to access, use, management of university data, devices and networks, it is noted that it has been moderately observed. Employees are generally complying with the guidelines set forth in this policy, which contributes to the overall security of university resources.

While the level of implementation is considered evident, it indicates that the university is on a positive trajectory in its efforts to protect data privacy and enhance cybersecurity. This moderate level of implementation offers a solid foundation for further strengthening security measures and ensuring the continued protection of sensitive data.

These findings also support the conclusions of some other study projects. An organizational information security environment significantly affects employees' threat assessment and coping skills, which in turn positively effects their cybersecurity compliance behavior [21]. Some of the challenges that organizations encounter in developing human knowledge to fight against social engineering attacks [22]. Also, some results revealed that despite of the state-of-the-art cyber security preparations and trained personnel, cybercriminals are still successful in their malicious acts of stealing sensitive data that is vital to organizations. This emphasized that organization with a strong information security culture were identified as having a mutual trust and integrity through the protection of their information [23]. In summary, these studies collectively indicate that while there are efforts to establish data privacy and cybersecurity in organizations, there are still challenges in implementation and enforcement that need to be addressed.

D. ***Level of Awareness of Data Privacy and Cybersecurity***

Table IV: Awareness of Data Privacy

Knowledge and Awareness of Data Privacy		
Statements	***Mean***	***Descriptive Value***
1. Awareness to general security	4.27	Fully Aware
2. Awareness to Information Security	4.21	Fully Aware
3. Awareness to Physical/Communications Systems Security	4.21	Fully Aware
Overall Weighted Mean	**4.23**	**Fully Aware**

Table IV shows the knowledge and awareness of the employees to data privacy which concerns their awareness to general security, information security and physical/communications systems security. For general security which include questions such as the need for a strong password, safeguarding themselves from social engineering, phishing, and cybercrime, non-disclosure of sensitive information to public places, using of trusted websites when browsing and downloading from the internet, opening email attachments and links, the employees revealed that they are fully aware

as shown in the computed mean of 4.27. This means that they have a high regard as to the measures to protect their data. For their awareness as to information security which include questions on their knowledge of sensitive information, proper methods for transmitting, storing, labeling and handling of sensitive information, encryption of sensitive data when sending it via email and in hardware and mobile devices, and posting sensitive data on social media sites, shows that employees are fully aware in protecting their personal information when using information communication systems as revealed in their mean of 4.21. And as to their awareness to physical/communications systems security, which include items on physical security procedures, malware protection, and secured storage for sensitive/critical data, shows that they are fully aware as reported in their mean of 4.21. The results show that the employees possess proficiency and knowledge on these measures as it is revealed in their overall weighted mean of 4.23.

Table V: Awareness of Cybercrime Prevention Acts

Knowledge and Awareness on the Cybercrime Prevention Acts		
Statements	***Mean***	***Descriptive Value***
1. Awareness as to the offenses against the confidentiality, integrity and availability of computer data and systems	4.13	Aware
2. Awareness as to Computer-related offenses	4.14	Aware
3. Awareness as to other cybercrimes	4.13	Aware
Overall Weighted Mean	**4.13**	**Aware**

Table 5 composed of the knowledge and awareness of the employees towards the dimensions of the Cybercrime Prevention Act of 2012 (RA10175) [24] which concerns on their awareness to the offenses against the confidentiality, integrity and availability of computer data and systems, awareness to computer-related offenses and other cybercrimes. Result shows that employees are aware of the cybercrime offenses as revealed in their overall weighted mean of 4.13. This means that they can adequately understand the issues which pertains to these measures.

In related studies conducted, similar findings were also found out on the level of awareness of employees to cybersecurity. [7] and [6] emphasizes the importance of engaging employees to proactively contribute to cybersecurity , starting with the design of cybersecurity policy and compliance plan. This further engage employees to be more aware of their organization's information security policy and procedures. Thus, these studies highlight the importance of enhancing employees' awareness of data privacy and cybersecurity acts, suggesting the need for coordinated planning, diverse strategies, engagement, and training to improve awareness.

E. Correlation Analysis of the Level of Awareness on Data Privacy and Cybersecurity to Profile Variables

Table VI: Result of Correlation Analysis of Data Privacy and Cybersecurity Awareness and Profile Variables

	Level of Awareness to Cybersecurity		**Level of Awareness to Cybersecurity**	
Variables	***Correlation Coefficient***	***Probability***	***Correlation Coefficient***	***Probability***
Profile				
Age	-.078	.196	.017	.777
Sex	-.007	.903	.017	.777
Civil Status	-.127*	.034	-.050	.408
Highest Educational Attainment	-.011	.849	-.060	.321
Designation	.040	.502	.055	.361
Position	-.057	.340	-.086	.154
Years in Service	-.160	.007	-.123*	039
Online Activities				
Number of hours of using internet	.006	.921	-.059	.329

Digital skills level	**.138***	.021	.034	.576
Digital devices used	.109	.069	.034	.571
Types of Connectivity	.055	.356	-.009	.880
Purpose of using the internet	.013	.825	.006	.914

In the result of correlation between the level of awareness of the employees to cybersecurity and their demographic profile, shown in Table VI, it was found out that there is a negative significant relation between the civil status and their awareness to cybersecurity, this implies that single employees tend to have the highest level of awareness about cybersecurity compared to married employees having a slightly lower level of awareness and widowed or separated employees having the lowest among the three groups. This negative association might suggest that marital status or personal life circumstances somehow influence an individual's awareness of cybersecurity. However, it is important to emphasize that correlation does not imply causality. Further comprehensive research would be necessary to fully understand the causes behind this finding, as additional elements or variables may be involved.

Also, the years in service of the employees was found out to be negatively significant to their awareness to cybersecurity and data privacy (Table VI). This must be attributed to various factors such as, employees who have been in the same role for many years may not have received the latest information and lack updated training, limited exposure to new technology which can result to lower awareness of current threats and in some cases, older employees may belong to a different generation that did not grow up with the same level of digital technology and cybersecurity awareness as younger generations.

For the correlation between the level of awareness to cybersecurity and their online activities, the employee's digital skills level, and their purpose of using the internet was positively correlated which means that the higher the level of skills of the respondents in using the internet, the higher is their awareness to cybersecurity. Several factors can explain this positive correlation, including increased familiarity with digital environments, which can make them more aware of potential cybersecurity risks and threats, as well as more hands-on experience with technology, which exposes them to a variety of digital security issues, making them more aware of the importance of cybersecurity practices.

According to certain studies, employees' level of understanding of data privacy and cybersecurity acts varies depending on their profile characteristics. Profile variables such as age, working industry, and education level all have a significant impact on information security policy awareness and compliance [15]. Also, employees who were aware of their company's cybersecurity policies were more competent in managing cybersecurity tasks [6]. Results from other studies discovered that gender influences security self-efficacy, prior experience, and computer skills, but has no effect on cues-to-action and self-reported cybersecurity activities [14]. These findings suggest that profile characteristics can influence employee understanding and compliance with data privacy and cybersecurity.

*F. **Correlation Analysis of the Extent of Implementation and Level of Awareness to Data Privacy and Cybersecurity***

Table VII: Correlation Analysis between the Extent of Implementation and Awareness of Employees to Data Privacy

Correlations			
			Implementation of Data Privacy
Spearman's rho	Implementation of Data Privacy	Correlation Coefficient	1.000
		Sig. (2-tailed)	.
	Awareness to General Security	Correlation Coefficient	.559**
		Sig. (2-tailed)	.000
	Awareness to Information Security	Correlation Coefficient	.628**
		Sig. (2-tailed)	.000
		Correlation Coefficient	.594**

	Awareness to Physical/Communications Systems Security	Sig. (2-tailed)	.000
**. Correlation is significant at the 0.01 level (2-tailed).			

Table VII shows the result of correlation analysis between the status of implementation and awareness of the employees to Data Privacy. It is very evident in the result that there is a strong correlation between the status of implementation and the level of awareness of the employees to data privacy as revealed in the table above.

Table VIII: Correlation Analysis between the Status of Implementation and Awareness of Employees to Cybersecurity

Correlations			
			Implementation of Cybersecurity
Spearman's rho	Implementation of Cybersecurity	Correlation Coefficient	1.000
		Sig. (2-tailed)	.
	Awareness to the Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems	Correlation Coefficient	.544**
		Sig. (2-tailed)	.000
	Computer-Related Offenses	Correlation Coefficient	.490**
		Sig. (2-tailed)	.000
	Other Cybercrime Offenses	Correlation Coefficient	.416**
		Sig. (2-tailed)	.000
**. Correlation is significant at the 0.01 level (2-tailed).			

For the correlation result of between the status of implementation and awareness to Cybersecurity of the employees, a strong correlation was also obtained as revealed in Table VIII.

This research study found a strong positive association between the status of implementation and employee awareness to data privacy and cybersecurity measures of the university. This suggests that as the university implements strong data privacy and cybersecurity protections, employees become more aware of these measures. This emphasizes the significance of a comprehensive approach to data privacy and cybersecurity policies within the university.

From the results of the relationship between the status of implementation and level of awareness of employees to data privacy and cybersecurity acts, related studies affirm that the findings of this study are related to the findings of some of the papers reviewed in this research [6] found out that employees' awareness of their company's information security procedures positively contributes to their cybersecurity compliance behavior. However, [25] found out on the study in Bangladesh that the general people are unaware of standard practices for cybersecurity and the government and respective organizations is not vibrant regarding cybercrime related issues. Also, [7] highlights that employees still lack awareness and conviction about their company's vulnerability to cybercrimes, indicating a need for improved cybersecurity awareness initiatives.

IV. CONCLUSION AND RECOMMENDATIONS

This study has explored a critical relationship between the employee awareness and the degree to which data privacy and cybersecurity measures are being implemented within an organization. The strong positive correlation identified highlights and potential for organization to improve and strengthen their data privacy and cybersecurity measures.

The findings provided some important insights. As organizations invest in complete cybersecurity implementation, employee awareness tends to rise. This association can be explained by a variety of factors, including improved digital skills through training and education, evident management support, periodic review and update of data privacy and cybersecurity measures to remain aligned with the evolving threats and best practices and allocation of sufficient

resources to support implementation of security policies. The result also benefits from positive feedbacks, in which improved security reduces incidents, which in turn encourages employees to emphasize the significance of security precautions.

Overall, this study provides practical understanding of the positive correlation between the extent of data privacy and cybersecurity implementation and employee awareness. Organizations that recognize and capitalize on this connection can strengthen their security measures, safeguard confidential and sensitive information, and develop a workforce that is security-aware.

ACKNOWLEDGMENT

The researchers would like to thank the RDE department of the university for the full support towards the completion of this study. We would like also to extend our sincerest gratitude to the administration for the fund granted to this research endeavor. Also, we are very grateful to the faculty and personnel of the university who willingly participated in the conduct of this study.

REFERENCES

[1] J. S. Averia et al., "Cybersecurity in the Philippines: Global Context and Local Challenges," The Lancet Psychiatry, vol. 7, no. 1, pp. 23–24, 2020.

[2] N. Ahmed, U. Kulsum, M. I. Bin Azad, A. S. Z. Momtaz, M. E. Haque, and M. S. Rahman, "Cybersecurity awareness survey: An analysis from Bangladesh perspective," 5th IEEE Reg. 10 Humanit. Technol. Conf. 2017, R10-HTC 2017, vol. 2018-Janua, pp. 788–791, 2018, doi: 10.1109/R10-HTC.2017.8289074.

[3] "Cybersecurity and Cybercrime-Philippine Perspective.pdf." .

[4] Interpol, "Cybercrime: Covid-19 Impact," Interpol, no. August, p. 20, 2020.

[5] S. Mamonov and R. Benbunan-Fich, "The impact of information security threat awareness on privacy-protective behaviors," Comput. Human Behav., vol. 83, pp. 32–44, 2018, doi: 10.1016/j.chb.2018.01.028.

[6] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," Int. J. Inf. Manage., vol. 45, no. October 2018, pp. 13–24, 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

[7] Kemper, "Improving employees' cyber security awareness," Comput. Fraud Secur., vol. 2019, no. 8, pp. 11–14, 2019, doi: 10.1016/S1361-3723(19)30085-5.

[8] N. P. Commission, "Republic Act No. 10173 - Data Privacy Act of 2012," Public Law, pp. 1–26, 2012.

[9] K. Demetzou, "Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation," Comput. Law Secur. Rev., vol. 35, no. 6, p. 105342, 2019, doi: 10.1016/j.clsr.2019.105342.

[10] Dang-Pham, S. Pittayachawan, and V. Bruno, "Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace," Comput. Human Behav., vol. 67, pp. 196–206, 2017, doi: 10.1016/j.chb.2016.10.025.

[11] M. Lubis and D. O. D. Handayani, "The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity," Procedia Comput. Sci., vol. 197, no. 2021, pp. 151–161, 2021, doi: 10.1016/j.procs.2021.12.129.

[12] M. J. Sule, M. Zennaro, and G. Thomas, "Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends," Technol. Soc., vol. 67, no. April, p. 101734, 2021, doi: 10.1016/j.techsoc.2021.101734.

[13] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," Comput. Secur., vol. 106, p. 102267, 2021, doi: 10.1016/j.cose.2021.102267.

[14] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors,"

Comput. Human Behav., vol. 69, pp. 437–443, 2017, doi: 10.1016/j.chb.2016.12.040.

[15] N. Chua, S. F. Wong, Y. C. Low, and Y. Chang, "Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations," Telemat. Informatics, vol. 35, no. 6, pp. 1770–1780, 2018, doi: 10.1016/j.tele.2018.05.005.

[16] Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," Comput. Ind., vol. 137, p. 103614, 2022, doi: 10.1016/j.compind.2022.103614.

[17] S. Hina, D. D. D. Panneer Selvam, and P. B. Lowry, "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world," Comput. Secur., vol. 87, p. 101594, 2019, doi: 10.1016/j.cose.2019.101594.

[18] Bozzon and G. Houben, "A Study of the Online Profile of Enterprise Users in Professional Social Networks," pp. 487–492, 2014.

[19] R. Patlolla, "A Study on Demographic Profile of Employees and Organizational Performance in Information Technology (IT) Sector from Select Region," vol. 4, no. October, pp. 10–21, 2018.

[20] R. Patlolla, M. R. Doodipala, and J. S. Managalagiri, "The Effect of IT Employees Demographic Profile on Sensitivity of Organizational Culture : A Study of Selected IT Companies in State Capital Region," pp. 1111–1119, 2017, doi: 10.4236/ajibm.2017.710079.

[21] L. Li, L. Xu, and W. He, "Computers in Human Behavior Reports The effects of antecedents and mediating factors on cybersecurity protection behavior," vol. 5, no. December 2021, 2022, doi: 10.1016/j.chbr.2021.100165.

[22] Aldawood and G. Skinner, "Challenges of implementing training and awareness programs targeting cyber security social engineering," Proc. - 2019 Cybersecurity Cyberforensics Conf. CCC 2019, no. Ccc, pp. 111–117, 2019, doi: 10.1109/CCC.2019.00004.

[23] Da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, "Defining organisational information security culture—Perspectives from academia and industry," Comput. Secur., vol. 92, p. 101713, 2020, doi: 10.1016/j.cose.2020.101713.

[24] "Rules_and_Regulations_Implementing_Republic_Act_10175.pdf.".

[25] N. Ahmed, U. Kulsum, M. I. Bin Azad, A. S. Z. Momtaz, M. E. Haque, and M. S. Rahman, "Cybersecurity awareness survey: An analysis from Bangladesh perspective," 5th IEEE Reg. 10 Humanit. Technol. Conf. 2017, R10-HTC 2017, vol. 2018-Janua, no. December 2019, pp. 788–791, 2018, doi: 10.1109/R10-HTC.2017.8289074.