GLOBAL JOURNAL
OF COMPUTER SCIENCE AND TECHNOLOGY - G: INTERDISCIPLINARY
Volume 26 | Issue 1 | 2026 Article ID: GJCST-256278 Language: English

CATALOGING
ACM • K.6.5, K.3.2 ARXIV • cs.CR, cs.CY DDC • 005.8

Level of Cybersecurity Awareness of Btech Employees: Basis for Proposing Cybersecurity Training

Article Record

Dr. Joseph L. Atayde[§*]
*Corresponding Author

Katherine V. Caballero[§]

Marielyn C. Icawat[§]

Jhon Michael D. Mariano[§]

Roel Mark R. Tagaan[§]

Mary Jane M. Toribio[§]

§ Institute of Business and Accountancy, Dalubhasaang Politekniko ng Lungsod ng Baliwag (BTECH), Baliwag, Philippines

RECEIVED	ACCEPTED	ONLINE PUBLISHED	PUBLISHED	PEER REVIEW
2026-04-17	2026-04-27	2026-06-23	2026-07-10	Double Blind

Abstract

Cybersecurity threats pose serious risks to the world, particularly in many educational institutions wherein they were handling, managing, and controlling large volume of sensitive data. Human errors remain a leading cause of data breaches, highlighting the importance of assessing the employees' level of cybersecurity awareness. This study aimed to determine the level of cybersecurity awareness of BTECH employees in terms of knowledge, skills, and attitude, and to examine whether there are significant difference and relationship among selected variables. Descriptive-quantitative research design with comparative and correlational components was utilized in this study. Data were collected from 190 teaching and nonteaching employees using a purposive sampling method. Gathering of data was accomplished through an adopted-modified and validated survey questionnaire. To analyze the data, percentage, frequency, weighted/composite mean, t-test, one-way ANOVA, and Pearson Product-Moment Correlation were used as statistical tools. Findings revealed a moderate level of cybersecurity awareness, with skills ranking highest (WM = 3.88), followed by attitude (WM = 3.47) and knowledge (WM = 3.29). A significant positive relationship was observed between knowledge, skills, attitude, and overall cybersecurity awareness. No significant differences were found across most demographic variables except for position. To significantly enhance and strengthen the cybersecurity knowledge, skills, and attitude of BTECH employees, this study concludes that proposing a cybersecurity training program is essential to improve cybersecurity awareness and reduce institutional vulnerability to cyberattacks.

attitude | cyberattacks | cybersecurity awareness | knowledge | skills

AI USE STATEMENT
No generative AI was used for analysis or results.

FUNDING
No external funding was declared for this work.

CONFLICT OF INTEREST
The authors declare no conflict of interest.

DATA AVAILABILITY
Not applicable for this article.

ETHICS
No ethics committee approval was required for this article type.

CONSENT
Not applicable for this article.

TRIAL REG.
Not applicable.

Crossref DOI: 10.34257/GJCSTG256278

How to Cite: Atayde et al. (2026). Level of Cybersecurity Awareness of Btech Employees: Basis for Proposing Cybersecurity Training. Global Journal of Computer Science and Technology, 26(1), 5-12. DOI: 10.34257/GJCSTG256278

METADATA CONTINUATION

AUTHOR CONTACT QR LEDGER

Dr. Joseph L. Atayde§*

Katherine V. Caballero§

Marielyn C. Icawat§

Jhon Michael D. Mariano§

Roel Mark R. Tagaan§

Mary Jane M. Toribio§

ARCHIVAL RECORD

GJCST · Vol 26 · Issue 1 · 2026

Article ID GJCST-256278 · DOI 10.34257/GJCSTG256278

Print ISSN 0975-4350 · Online ISSN 0975-4172

Global Journal of Computer Science and Technology - Section G
GJCST Volume 26 Issue 1

Level of Cybersecurity Awareness of Btech Employees: Basis for Proposing Cybersecurity Training

Dr. Joseph L. Atayde[§*], Katherine V. Caballero[§], Marielyn C. Icawat[§], Jhon Michael D. Mariano[§], Roel Mark R. Tagaan[§], and Mary Jane M. Toribio[§]

Affiliations
§ Institute of Business and Accountancy, Dalubhasaang Politekniko ng Lungsod ng Baliwag (BTECH), Baliwag, Philippines

Abstract

Cybersecurity threats pose serious risks to the world, particularly in many educational institutions wherein they were handling, managing, and controlling large volume of sensitive data. Human errors remain a leading cause of data breaches, highlighting the importance of assessing the employees' level of cybersecurity awareness. This study aimed to determine the level of cybersecurity awareness of BTECH employees in terms of knowledge, skills, and attitude, and to examine whether there are significant difference and relationship among selected variables. Descriptive-quantitative research design with comparative and correlational components was utilized in this study. Data were collected from 190 teaching and nonteaching employees using a purposive sampling method. Gathering of data was accomplished through an adopted-modified and validated survey questionnaire. To analyze the data, percentage, frequency, weighted/composite mean, t-test, one-way ANOVA, and Pearson Product-Moment Correlation were used as statistical tools. Findings revealed a moderate level of cybersecurity awareness, with skills ranking highest (WM = 3.88), followed by attitude (WM = 3.47) and knowledge (WM = 3.29). A significant positive relationship was observed between knowledge, skills, attitude, and overall cybersecurity awareness. No significant differences were found across most demographic variables except for position. To significantly enhance and strengthen the cybersecurity knowledge, skills, and attitude of BTECH employees, this study concludes that proposing a cybersecurity training program is essential to improve cybersecurity awareness and reduce institutional vulnerability to cyberattacks.

Keywords: *attitude, cyberattacks, cybersecurity awareness, knowledge, skills*

*** Corresponding Author**
Dr. Joseph L. Atayde

DOI
10.34257/GJCSTG256278

1. Introduction

Technology plays a significant role in modern organizations, like educational institutions as it enhances the efficiency of communication, efficiency, and data management. While facing the advantages and reliance of educational institutions into digital systems, it also exposes institutions to cyberattacks such as phishing, ransomware, and unauthorized access.

Huge amounts of confidential information such as documents, records, and data were controlled and managed by educational institutions. Because of factors mentioned, educational institutions become frequent targets of cyberattacks. Studies and reports indicate that human error is one of the primary causes of data breaches, emphasizing the importance of employee awareness and cybersecurity practices.

In the Philippine context, rapid digitalization in education has further increased exposure to cyber risks. Despite technological advancements, gaps in employee awareness and training remain a concern. Therefore, assessing cybersecurity awareness is essential to identify vulnerabilities and develop effective training programs.

Cybersecurity awareness in this study is viewed as a multidimensional construct consisting of knowledge, skills, and attitude, while demographic variables serve as possible influencing factors. Additionally, selected demographic variables may serve as intervening factors that can influence the level of cybersecurity awareness of employees.

1.1. Review of Related Literature

Human error plays a critical role in cyberattacks, often due to negligent employee actions that lead to data breaches. Research, including AlKuwari (2024), emphasizes inadequate training and awareness as major contributors to these threats, particularly concerning social engineering tactics like phishing. The National Privacy Commission of the Philippines identifies human error as a primary cause of data breaches in sectors like education, highlighting the necessity for institutions to implement protective measures and comply with the Data Privacy Act of 2012 (RA 10173). Furthermore, Martínez-Peláez et al. (2024) demonstrate that improved cybersecurity training can reduce employee susceptibility to attacks, stressing the importance of integrating cybersecurity education into regular operations.

Moreover, the research highlights that understanding human factors is essential, as employees can be both an organization's greatest asset and its weakest link in terms of cybersecurity. Nonum et al. (2025) argue that organizations often overlook the importance of employee behavior and decision-making in cybersecurity, leading to vulnerabilities that attackers exploit through trust and authority.

Despite advancements in technical safeguards, human error, particularly in phishing attacks, remains a critical concern, as noted by Alqahtani and Alshahrani (2021). Phishing is a prevalent method of cyberattacks, exploiting cognitive biases and a lack of awareness among employees, which can lead to severe consequences such as data theft and ransomware. This highlights the necessity for organizations to adopt a human-centered cybersecurity strategy that encompasses behavioral science to effectively complement existing technical defenses.

In recent incidents of data breaches involving educational institutions, the University of the Philippines Tacloban College (UPTC) experienced a breach of its Learning Management System, compromising over 1,600 student records. UPTC has implemented preventive actions with guidance from UP Diliman, while the UP System introduced privacy guidelines. Pamantasan ng Lungsod ng Maynila's official Facebook page was hacked due to phishing, prompting alerts from the Manila City Government. Romblon State University reported a breach leaking sensitive information, leading to collaborations with law enforcement and cybersecurity strategies. Similarly, BTECH's Facebook Admissions page faced unauthorized access, and Ifugao State University experienced hacking incidents, calling for improved cybersecurity measures. The Department of Education's Ilocos Norte Division reported a breach affecting three million records, stressing the need for enhanced cybersecurity training in educational institutions.

Ongoing training and simulations are crucial for reducing phishing risks and enhancing cybersecurity awareness among employees. A study by Toth (2025) found that continuous training can reduce phishing attacks by 50% within six months. Customized training targeting specific departments is also essential, as evidenced by Alenzi and Rusho (2024), which indicated that tailored training can reduce human error incidents by $45\% - 65\%$, particularly in non-technical departments lacking cybersecurity knowledge.

Further research by Roy and Francis (2023) highlighted that persistent training diminishes data breaches by addressing human-related factors. Additionally, structured awareness training significantly influences employee behavior, leading to fewer phishing and data mishandling incidents, as noted by Hadlington and Parsons (2021). Creating a supportive training environment that considers cultural factors and using engaging simulation exercises can enhance employee alignment with cybersecurity principles while making learning enjoyable.

1.2. Statement of the Problem

This study aims to determine the level of cybersecurity awareness among teaching and non-teaching BTECH employees and to examine whether significant differences and relationships exist among selected variables. The study was specifically designed to address the questions listed below:

1. What is the profile of BTECH employees in terms of:
    a. Age
    b. Sex
    c. Position
    d. Nature of work
    e. Employment status, and
    f. Length of service?
2. What is the level of cybersecurity awareness of employees in terms of:
    a. Knowledge
    b. Skills, and
    c. Attitude?
3. Is there a significant difference in the level of cybersecurity awareness of employees when grouped according to selected demographic variables such as age, sex, position, nature of work, employment status or length of service?
4. Is there a significant relationship among employees' cybersecurity knowledge, skills, and attitudes with their overall level of cybersecurity awareness?
5. What cybersecurity training programs may be proposed to address the needs of BTECH employees in terms of cybersecurity?

1.3. Null Hypothesis (H_0)

1. There is no significant difference in the level of cybersecurity awareness of employees when grouped according to age, sex, position, nature of work, employment status, and length of service.
2. There is no significant relationship between employees' level of cybersecurity awareness and their cybersecurity knowledge, skills and attitudes.

1.4. Alternative Hypothesis (H_1)

1. There is a significant difference in the level of cybersecurity awareness of employees when grouped according to age, sex, position, nature of work, employment status, and length of service.
2. There is a significant relationship between employees' level of cybersecurity awareness and their cybersecurity knowledge, skills and attitudes.

1.5. Theoretical and Conceptual Framework

This study examines the intersection of individual behaviors, organizational practices, and attitudes towards cybersecurity, positing that employees' actions are influenced by their knowledge, skills, and attitudes regarding cyber threat protection. It references the Unified Learning Model (ULM) which suggests that various factors, such as prior knowledge, motivation, and cognitive processing, shape how individuals acquire and utilize knowledge. The ULM implies that an employee's cybersecurity awareness increases through training and practical experience with institutional systems and tasks.

Additionally, Protective Motivation Theory (PMT) is highlighted, explaining how individuals protect themselves from perceived threats by evaluating the severity and likelihood of those threats (Threat Appraisal) and their ability to respond (Coping Appraisal). The study indicates that employees' cybersecurity knowledge relates to their awareness of potential cyberattacks and that their skills are indicative of their confidence in employing protective measures. Finally, the study introduces a conceptual framework linking cybersecurity awareness to three vital factors: knowledge (understanding of cybersecurity concepts), skills (ability to apply protective measures), and attitude (perceptions and responsibility towards cybersecurity). A positive attitude enhances the likelihood of adopting precautionary security behaviors.

Figure 1 illustrates the input-process-output (IPO) model in the context of cybersecurity employee training. The input includes

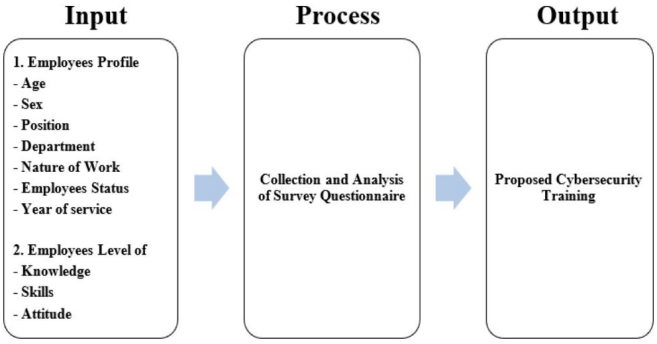

Figure 1. Paradigm of the Study

employee profiles along with their knowledge, skills, and attitudes regarding cybersecurity. The process involves the distribution of surveys and statistical analysis aimed at identifying relationships among these variables. The study's findings catalyzed the formulation of a proposed cybersecurity training program, the main output of this research. This program seeks to enhance participants' knowledge, bolster their cybersecurity skills, and foster a positive attitude towards cybersecurity, ultimately improving their overall cybersecurity awareness. According to IBM Security (2025), organizations that provide cybersecurity training and educate their employees about various cyberattacks are less likely to experience significant data breaches, thereby highlighting the critical role of human factors in cybersecurity.

2. Method

2.1. Research Design

This study employed a descriptive-quantitative design with comparative and correlational elements to assess the cybersecurity awareness of BTECH employees regarding their knowledge, skills, and attitudes.

The descriptive approach generated an overview of employees' understanding of sensitive data usage, information protection, password management, and cyberattack identification. Utilizing a Likert scale, the research evaluated employees' knowledge, skills and attitude. While the comparative aspect investigated differences in awareness across demographic variables such as age, sex, and length of service, analyzed using the independent samples t-test and ANOVA.

Additionally, the study explored correlations between employees' knowledge, skills, attitudes, and overall cybersecurity awareness via the Pearson Product-Moment Correlation Coefficient, ultimately providing insights into factors influencing cybersecurity readiness among BTECH employees.

2.2. Respondents/Participants

The respondents consisted of 190 teaching and non-teaching BTECH employees who are exposed to digital systems and institutions data. This study utilized purposive sampling, this approach ensures that the respondents were relevant to the research objectives by giving accurate information about their current cybersecurity knowledge, skills, and attitudes.

Before obtaining the data needed from the respondents, the researchers informed them regarding the objective of study and asked for their consent. Respondents who declined participation were excluded, while responses found to be invalid or incomplete were removed and not considered in the final analysis. This thorough selection process makes sure that the information mirrors the engagement of employees who are actively engaged with the institution's digital system and sensitive information.

2.3. Questionnaire/Survey Tool

An adopted-modified version of a validated research questionnaire by Nikel and Amaechi (2021) was utilized to assess BTECH employees' cybersecurity awareness, encompassing their knowledge, skills, and attitudes. Following modifications, the questionnaire was validated by three experts, each with advanced qualifications in relevant fields. Feedback was solicited based on criteria such as clarity, organization, and content adequacy, leading to further enhancements of the instrument to align with the research objectives.

A pilot study involving 30 teaching and non-teaching employees (not the actual respondents of the study) was conducted to evaluate the questionnaire's reliability, internal consistency, and clarity, providing insights for refinements prior to the main study. The instrument aimed to gauge employees' knowledge of cybersecurity, their skills in safeguarding institutional data, and their attitudes towards cybersecurity practices. It specifically assessed understanding of cyberattacks, security policies, and principles of data protection, alongside practical skills like secure password management and safe handling of sensitive information.

Furthermore, the instrument measured attitudes towards cybersecurity, highlighting responsibility, risk awareness, and compliance with security measures. The methodology employed a Likert Scale format for responses, facilitating easy analysis and ensuring reliability and validity based on respondents' perceptions, ultimately offering a thorough evaluation of cybersecurity awareness within the institution.

Table 1. Subscale Scoring. Each dimension contains 10 items

Dimension	Item Numbers	Possible Score Range
Knowledge	1-10	10-50
Skills	11-20	10-50
Attitudes	21-30	10-50
Overall Cybersecurity Awareness	1-30	30-150

2.4. Scoring Method

Table 2. Interpretation of Scores per Dimension (Knowledge / Skill / Attitudes)

Score Range	Interpretation
1.00 - 2.30	Low Level
2.40 - 3.60	Moderate Level
3.70 - 5.00	High Level

Table 3. Overall Cybersecurity Awareness Interpretation

Score Range	Level of Awareness
1.00 - 2.30	Low
2.33 - 3.63	Moderate
3.67 - 5.00	High

2.5. Validation of the Instrument

When all 30 items were analyzed collectively, the instrument obtained a Cronbach's Alpha of 0.86, indicating good internal consistency. An alpha coefficient above 0.70 suggests that the items

are correlated and consistently measure the intended constructs. This result confirms that the questionnaire is reliable and suitable for use in the study. Table 4 shows the reliability per construct.

Table 4. Reliability Per Construct

Construct	No. of Items	Cronbach's Alpha	Interpretation
Knowledge	10	0.78	Acceptable
Skills	10	0.84	Good
Attitude	10	0.95	Excellent
Overall	30	0.86	Good Internal Consistency

The reliability analysis results, as presented in Table 4, demonstrate an overall Cronbach's alpha coefficient of 0.86 for the instrument, indicating good internal consistency. This suggests that the items within the constructs of knowledge, skills, and attitude reliably measure the intended constructs. Among these dimensions, attitude exhibited the highest reliability with a coefficient of 0.95, followed by skills at 0.84 and knowledge at 0.78. All reliability values surpass the minimum acceptable threshold of 0.70, confirming the instrument's statistical reliability for both research and academic purposes.

3. Results and Discussion

This chapter presents the data gathered from the respondents, along with the analysis and interpretation of the results. The data were obtained through a survey questionnaire distributed to both teaching and non-teaching employees of BTECH. The presentation of data is organized according to the objectives of the study, which include the profile of the respondents, the level of cybersecurity knowledge, skills, and attitude, and the relationship between variables.

The researchers analyzed the profiles of the participants based on several criteria, including age group, sex, position, nature of work, employment status, and length of service. Additional details such as the type of device used for work, the amount of cybersecurity training received, the frequency of attending training, and the level of familiarity with institutional cybersecurity policies were included in the survey instrument.

Table 5. Distribution of Respondents According to Age

Age	Frequency	Percentage
21-30 years old	30	15.79%
31-40 years old	66	34.74%
41-50 years old	69	36.32%
51-60 years old	17	8.95%
61 and above	8	4.21%
Total	190	100%

Table 5 shows that most respondents are 41-50 years old (69 respondents, 36.32%), followed closely by 31-40 years old (66 respondents, 34.74%). Respondents aged 21-30 years accounted for 15.79% (30 respondents), 51-60 years for 8.95% (17 respondents), and only 4.21% (8 respondents) were 61 years and above. This distribution reflects the workforce composition of BTECH, where mid-career employees dominate.

The majority of respondents were female (105 respondents, 55.26%), while males comprised 44.74% (85 respondents). Including sex as a demographic variable is important for analyzing potential differences in workplace behavior and cybersecurity awareness (Robbins & Judge, 2017).

Most respondents were faculty members (139 respondents, 73.16%), followed by administrative staff (41 respondents, 21.58%).

Table 6. Distribution of Respondents According to Sex

Sex	Frequency	Percentage
Male	85	44.74%
Female	105	55.26%
Total	190	100%

Table 7. Distribution of Respondents According to Position

Position	Frequency	Percentage
Head Office	7	3.68%
Program Director	3	1.58%
Administrative	41	21.58%
Faculty	139	73.16%
Total	190	100%

Head Office personnel accounted for 7 respondents (3.68%), while Program Directors were the smallest group with 3 respondents (1.58%).

Table 8. Distribution of Respondents According to Nature of Work

Nature of Work	Frequency	Percentage
Teaching	152	80%
Non-Teaching	38	20%
Total	190	100%

A majority of respondents (152 respondents, 80%) were engaged in teaching-related work, while 38 respondents (20%) performed non-teaching tasks. Teaching employees frequently interact with computers, institutional databases, and online platforms, highlighting their relevance in assessing cybersecurity knowledge and practices (DoE, 2020; Flores, 2025).

Table 9. Distribution of Respondents According to Length of Service

Years of Service	Frequency	Percentage
Less than 1 year	4	2.11%
1-2 years	25	13.16%
3-4 years	71	37.37%
5 years and above	90	47.37%
Total	190	100%

Respondents with 5 or more years of service comprised 47.37% (90 respondents), followed by those with 3-4 years at 37.37% (71 respondents). This indicates that employees generally stay long-term in the institution, likely due to job stability, organizational support, and job satisfaction (Camlian & Baron, 2025; Anog, 2024).

Table 10. Distribution of Respondents According to Employment Status

Employment Status	Frequency	Percentage
Permanent	85	44.74%
Part-Time	105	55.26%
Total	190	100%

Most respondents were part-time employees (105 respondents, 55.26%), while permanent employees comprised 44.74% (85 respondents). Including both groups provides a broader understanding of cybersecurity awareness (Pugong, 2025).

The majority of respondents primarily used desktop computers (97 respondents, 51.05%), followed by laptops (69 respondents, 36.32%) and tablets (24 respondents, 12.63%).

Table 11. Distribution of Respondents According to Device Used

Device Used	Frequency	Percentage
Desktop	97	51.05%
Laptop	69	36.32%
Tablet	24	12.63%
Total	190	100%

Table 12. Distribution of Respondents According to Attendance in Cybersecurity Training

Attended Training	Frequency	Percentage
Yes	88	46.32%
No	102	53.68%
Total	190	100%

Out of 190 respondents, 88 (46.32%) reported having attended cybersecurity training, while 102 (53.68%) had not. This highlights a gap in formal cybersecurity education.

Table 13. Distribution of Respondents According to Frequency of Training Attendance

Frequency of Training	Frequency	Percentage
Never	102	53.68%
Once a year	52	27.37%
Twice a year	26	13.68%
Frequently (3+ per year)	10	5.26%
Total	190	100%

Among respondents, 53.68% (102) had never attended training. This demonstrates low participation in regular cybersecurity training.

Table 14. Awareness of Existing Cybersecurity Policy in the Institution

Aware of Policy	Frequency	Percentage
Yes	85	44.74%
No	105	55.26%
Total	190	100%

A majority, 105 respondents (55.26%), reported not being aware of the institution's cybersecurity policy.

Table 15. Familiarity with Existing Cybersecurity Policy in the Institution

Familiarity Level	Frequency	Percentage
Not Familiar / Never heard	105	55.26%
Slightly Familiar	44	23.16%
Familiar	36	18.95%
Very Familiar	5	2.63%
Total	190	100%

The majority of respondents (105, 55.26%) were not familiar with the policy.

The overall composite mean for knowledge was 3.29 (moderate). Respondents demonstrated high awareness of general practices but remained neutral on technical aspects like firewalls and antivirus updates.

The composite mean for skills was 3.88 (high). Respondents expressed strong recognition of the need for training.

The overall composite mean for attitude was 3.47 (moderate). Respondents showed a positive attitude regarding shared responsibility.

Table 16. Weighted Mean for Cybersecurity Knowledge of BTECH Employees

Statement	WM	Interpretation
1. I have prior knowledge about cyberattacks.	3.01	Neutral
2. I have sufficient information about cybersecurity policies and procedures.	3.10	Neutral
3. My organization practiced multi-factor authentication.	2.83	Neutral
4. My office device is connected to the internet.	4.37	Strongly Agree
5. I know whether my device has an enabled firewall.	2.65	Neutral
6. I know how to check if my device has an updated anti-virus.	2.72	Neutral
7. I am the only person who has access to passwords for my work-related accounts.	3.17	Neutral
8. I use different passwords for everything that requires a password.	3.09	Neutral
9. I only open email attachments from trusted or verified sources.	3.67	Agree
Overall Composite Mean	**3.29**	**Moderate**

Table 17. Weighted Mean for Cybersecurity Skills of BTECH Employees

Statement	WM	Interpretation
1. I feel confident handling cybersecurity threats.	3.17	Neutral
2. I am open to attending cybersecurity training programs.	3.87	Agree
3. Cybersecurity training is important for my job.	3.81	Agree
4. I need training on identifying phishing emails and messages.	4.07	Agree
5. I need training on how to prevent malware infections.	3.94	Agree
6. I need training on how to respond to ransomware attacks.	4.00	Agree
7. I need training on creating and managing strong passwords.	4.02	Agree
8. I need training on protecting personal and institutional data.	4.16	Agree
9. I need training on safe internet and email usage.	3.88	Agree
10. I think regular training can reduce successful cyberattacks.	3.89	Agree
Overall Composite Mean	**3.88**	**High**

Table 18. Cybersecurity Attitude of BTECH Employees

Statement	WM	Interpretation
1. Management responsibility to ensure organization is protected.	3.99	Agree
2. Existing computer systems already provide enough protection.	3.32	Neutral
3. IT security is a priority within my organization.	3.33	Neutral
4. Reporting a cyberattack is a responsibility of every employee.	4.15	Agree
5. I am confident that I would be able to spot signs of a cyberattack.	3.23	Neutral
6. I can help protect my organization from cyberattacks.	3.50	Agree
7. Cybercriminals may be more knowledgeable than people protecting us.	3.02	Neutral
8. Cybercriminals only target a company for financial gain.	3.23	Neutral
9. Cybersecurity is a public safety issue.	3.64	Agree
10. Mistakes or violations are disciplined or penalized.	3.28	Neutral
Overall Composite Mean	**3.47**	**Moderate**

Table 19. Overall Cybersecurity Awareness Summary

Dimension	Overall Mean	Interpretation
Knowledge	3.29	Moderate Level
Skills	3.88	High Level
Attitude	3.47	Moderate Level
Grand Weighted Mean	**3.55**	**Moderate Awareness**

The grand mean was 3.55 (moderate). Skills ranked highest, followed by attitude and knowledge.

Table 20. T-Test comparing Awareness based on Sex

Sex	N	Mean	SD	t-value	df	p-value	Decision
Male	85	3.284	0.474	-0.142	188	0.887	Fail to Reject H_0
Female	105	3.293	0.474				

There was no significant difference in cybersecurity awareness based on sex ($p = 0.887$).

Table 21. T-Test Comparing Awareness between Teaching and Non-Teaching Employees

Nature of Work	N	Mean	SD	t-value	df	p-value	Decision
Teaching	152	3.311	0.465	1.300	188	0.195	Fail to Reject H_0
Non-Teaching	38	3.200	0.498				

Awareness is consistent across teaching and non-teaching employees ($p = 0.195$).

Employment status does not significantly influence cybersecurity awareness ($p = 0.486$).

No significant differences in cybersecurity awareness among different age groups ($p = 0.287$).

Table 22. T-Test Comparing Awareness between Permanent and Part-Time Employees

Employment Status	N	Mean	SD	t-value	df	p-value	Decision
Permanent	85	3.262	0.497	-0.697	188	0.486	Fail to Reject H_0
Part-Time	105	3.310	0.453				

Table 23. One-Way ANOVA across Different Age Groups

Age Group	N	Mean	SD	F/p-value	Decision
21-30	30	3.20	0.48	1.26	Fail to Reject H_0
31-40	66	3.33	0.49	(p=0.287)	
41-50	69	3.30	0.48		
51-60	17	3.39	0.26		
61 and above	8	3.01	0.57		

Table 24. One-Way ANOVA Comparing Awareness across Different Positions

Position	N	Mean	SD	F/p-value	Decision
Head Office	7	2.97	0.60	4.08	Reject H_0
Program Director	3	2.83	0.42	(p=0.008)	
Administrative	41	3.16	0.43		
Faculty	139	3.35	0.47		

There is a significant difference in cybersecurity awareness based on employees' positions ($p = 0.008$).

Table 25. One-Way ANOVA based on Length of Service

Length of Service	N	Mean	SD	F/p-value	Decision
< 1 year	4	3.53	0.42	1.15	Fail to Reject H_0
1-2 years	25	3.33	0.37	(p=0.331)	
3-4 years	71	3.16	0.56		
5+ years	90	3.29	0.45		

No significant difference in awareness based on length of service ($p = 0.331$).

Table 26. Correlation Matrix (Relationship among Knowledge, Skills, Attitude, and Awareness)

Variables	Knowledge	Skills	Attitude	Awareness
Knowledge	1.000	0.58**	0.61**	0.62**
Skills	0.58**	1.000	0.66**	0.74**
Attitude	0.61**	0.66**	1.000	0.68**
Awareness	0.62**	0.74**	0.68**	1.000

Correlation analysis indicated a significant positive relationship between overall cybersecurity awareness and each dimension. Skills showed the strongest association with overall awareness.

The study employs the Unified Learning Model (ULM) and Protection Motivation Theory (PMT) to interpret findings. It reveals that awareness is more significantly shaped by common institutional experiences than by demographic factors. Differences between job positions highlight that role impacts exposure to cybersecurity tasks. The findings underscore the necessity for structured and ongoing training programs that enhance knowledge, skills, and attitudes effectively.

4. Conclusion

A moderate level of cybersecurity awareness among BTECH employees was revealed in this study. While employees generally demonstrate positive attitudes toward cybersecurity practices, there are still gaps in their knowledge and skills that may increase susceptibility to cyberthreats.

Furthermore, the significant relationship among knowledge, skills, attitude, and overall cybersecurity awareness emphasizes the importance of strengthening these factors to enhance employees' preparedness. Additionally, the relationship between these dimensions confirms that cybersecurity awareness is multidimensional. The results also suggested a significant knowledge gap regarding training and policies, as the majority had never had formal training and were unfamiliar with institutional guidelines.

Given these findings, to enhance employees' cybersecurity awareness and promote responsible digital behavior, this study proposes a structured cybersecurity training program. This program can contribute to the improvement of the institution's cybersecurity posture and minimize risks associated with cyberattacks. This highlights the need for making policies more accessible and providing structured training to address the knowledge gap.

This study is limited to employees of a single institution, which may restrict the generalizability of the findings. Future studies may explore additional factors influencing cybersecurity awareness and assess the effectiveness of proposed training programs within the organization.

■ ACKNOWLEDGMENT

The researchers would like to express their sincere gratitude to all the individuals who contributed to the successful completion of this research study.

First and foremost, the researchers extend their deepest appreciation to their research adviser, Mr. Jared P. Manalastas, LPT, MAED, for his guidance throughout the conduct of this study.

The researchers also express their heartfelt gratitude to Dr. Ma. Socorro N. Bartolom, DBA, CPA, Dean of the Institute of Business and Accountancy, for sharing her expertise to the researchers for the development of this study.

Sincere appreciation is also extended to Prof. Al-Lawrence G. Cruz, Vice President for Administration and Finance; Ms. Aida S. Ramos, Ed.D., Vice President for Academic Affairs and Research; Ms. Reina Rodie Lyn Cruz, LPT, Ms. Danica G. Camarino, Mr. John Nicole S. Vizcarra, and Atty. Marynelle A. Salinas-De Jesus, for their assistance in facilitating the dissemination of the survey questionnaires to the respondents of the study.

The researchers would also like to thank Mr. Renz Allan V. Canlas, MIT, for generously sharing his knowledge in information technology, which greatly contributed to this research.

Special thanks are extended to Ms. Ma. Niña I. Adriano, MPA, MALLE, for her significant assistance and valuable contributions that greatly helped in the completion of this study.

Heartfelt gratitude is also extended to Ms. Angelica F. Cando and Ms. Jonabeth B. Ingaran for their assistance that greatly contributed to the success of this study.

Sincere appreciation is given to Mr. Jhed Ting for the generous financial support extended throughout the conduct of this study.

The researchers likewise express their sincere appreciation to the teaching and non-teaching employees of BTECH for their voluntary participation and meaningful contribution to the successful completion of this research.

Above all, the researchers offer their deepest gratitude to God Almighty for granting them wisdom, strength, and guidance throughout the entire research process.

■ REFERENCES

[1] Abubakar, A. M., Elrehail, H., Alatailat, M. A., & Elçi, A. (2019). Knowledge management innovation, and organiza-

tional performance: A study of SMEs in developing countries. *Journal of Innovation & Knowledge*, 4(2), 104-114. https://tinyurl.com/8e3m7pad

[2] AlKuwari, R. (2024). Enhancing cybersecurity awareness training for mitigating human-induced cybersecurity breaches. *International Journal of Engineering and Computer Science*. https://ijecs.in/index.php/ijecs/article/view/4917

[3] Alenzi, M. A. S., & Rusho, M. A. (2024). A field study on the impact of the level of knowledge of Human Resources employees about the principles and applications of cybersecurity on Human Resources laws. *International Journal of Intelligent Systems and Applications in Engineering*. https://ijisae.org/index.php/IJISAE/article/view/883

[4] Anog, M. D. I. (2024). Examining teacher retention through the lens of job satisfaction and school commitment in a private school in Cebu, Philippines. *International Journal of Learning, Teaching and Educational Research*. https://ijlter.org/index.php/ijlter/article/view/11243

[5] Asido, D. (2024, January 8). Ifugao State U taps DICT, Meta to retake FB page from hackers. *The Post*. https://thepost.net.ph/news/campus/ifugao-state-u-taps-dictmeta-to-retake-fb-page-from-hacker

[6] Camlian, M. M., & Baron, J. V. (2025). Workplace health and safety, social support, and turnover intention in private higher education institutions in the Philippines. *Annals of Human Resource Management Research*, 5(1), 1-14. https://tinyurl.com/4372vbuv

[7] Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approach* (5th ed.). SAGE Publications. https://collegepublishing.sagepub.com/products/research-design-6-270550

[8] Clubb, A. C., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, 28(3), 231-247. https://tinyurl.com/4w5vubaa

[9] Daily Dark Web. (2025, October 7). DepEd Ilocos Norte data breach exposes 3 million records. https://dailydarkweb.net/deped-ilocos-norte-data-breach-exposes-3-million-records/

[10] Department of Education. (2020). DepEd Order No. 018, s. 2020: Policy guidelines for the provision of learning resources in the implementation of the basic education learning continuity plan. https://www.deped.gov.ph/2020/07/20/july-20-2020-do-018-s-2020-policy-guidelines-for-the-provision-of-learning-resources-in-the-implementation-of-the-basic-education-continuity-plan

[11] Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBiS). *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2873-2882. https://doi.org/10.1145/2702123.2702249

[12] ENISA. (2022). Cybersecurity threats for social media platforms. *European Union Agency for Cybersecurity*. https://www.enisa.europa.eu/topics/csirt-cert-services/social-media-security

[13] Nonum, E. O., Avwokuruaye, O., & Umar, A. M. (2025). Social Engineering: Understanding Human Factors In Cyber Security. *International Journal of Convergent and Informatics Science Research*, 7(9). https://doi.org/10.70382/hijcisr.v07i9.032

[14] Facebook, Inc. [Meta Platforms]. (2021, April). Facebook data breach exposes 533 million users. https://www.facebook.com/meta/news/data-breach-2021

[15] Gil, M. (2024, April 30). Romblon State U assesses data breach after website hacking. *Philippine News Agency*. https://www.pna.gov.ph/articles/1223765

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

[17] Hadlington, L. (2018). Employees' attitudes towards cybersecurity and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Information Security*, 17(3), 285-297. https://doi.org/10.1007/s10207-017-0372-0

[18] IBM Security. (2025). Cybersecurity trends and breach prevention report. IBM. https://www.ibm.com/security/data-breach

[19] Ifugao State University. (2025, June 25). Univ takes proactive steps to bolster data privacy, and kicks-off manual development. https://www.ifsu.edu.ph/postview/

[20] Ifugao State University. (2024, September 12). University personnel trained on cybersecurity in DICT workshop [News release]. https://www.ifsu.edu.ph/postview/

[21] Interaksyon. (2024, December 9a). Manila PIO takes on PLM announcements as the university's Facebook gets hacked. https://interaksyon.philstar.com/trends-spotlights/2024/12/09/288402/manila-pio-plm-announcements-facebook-hacked/

[22] Interaksyon. (2024, December 9b). PLM Facebook page hacked, renamed by attackers. https://interaksyon.philstar.com/trends-spotlights/2024/12/09/288402/manila-pio-plm-announcements-facebook-hacked

[23] International Journal of Research Publication and Reviews. (2025). The 21st century ICT-based skills and pedagogical practices of public elementary school teachers in Cotabato Province. https://ijrpr.com/uploads/V6ISSUE6/IJRPR48309.pdf

[24] ISACA. (2023). Cybersecurity leadership and organizational support guidelines. https://www.isaca.org/resources

[25] Johnston, A., Siponen, M., & Warkentin, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-134. https://doi.org/10.2307/24670461

[26] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, 52, 194-206. https://doi.org/10.1016/j.cose.2015.02.003

[27] Kaur, R., & Singh, P. (2022). Data privacy and access control vulnerabilities in social media platforms: A study on Facebook. *Journal of Cybersecurity and Information Management*, 15(3), 45-60.

[28] Kruger, H. A., & Kearney, W. D. (2005). A prototype for assessing information security awareness. *Computer and Security*, 25(4), 289-296. https://doi.org/10.1016/j.cose.2005.10.001

[29] Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

[30] Martínez-Peláez, R., Velarde-Alvarado, P., Félix, V. G., Ochoa-Brust, A., Ostos, R., & Mena, L. J. (2024). Assessing employee susceptibility to cybersecurity risks. *International Journal of Information Security and Privacy*, 18(1). https://doi.org/10.4018/IJISP.2024010101

[31] Nash, J. (2022). Cyberattacks on critical infrastructure: Lessons from recent incidents. *Journal of Critical Infrastructure Security*, 14(1), 23-41.

[32] NIST. (2003). Building an information technology security awareness and training program (SP 800-50). https://csrc.nist.gov/pubs/sp/800/50/final

[33] National Privacy Commission. (2021, April 15). NPC validation of compromised Facebook accounts in the Philippines. https://privacy.gov.ph/npc-investigating-alleged-large-scale-facebook-breach

[34] National Privacy Commission. (2022). Annual report on personal data protection and breaches in the education sector. https://www.privacy.gov.ph

[35] National Privacy Commission. (2024). Breach notification report 2022-2024: Trends and causes across sectors. https://www.privacy.gov.ph

[36] National Privacy Commission. (2025). Annual security incident reporting (ASIR) and data breach causes. https://philippines.incorp.asia/guides/annual-security-incident-reporting/

[37] Ng, T. W. H., & Feldman, D. C. (2010). The relationships of age with job attitudes: A meta-analysis. *Personnel Psychology*, 63(3), 677-718. https://onlinelibrary.wiley.com/doi/10.1111/j.1744-6570.2010.01184.x

[38] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

[39] Peters, J. (2023, November 30). Human error is responsible for 74% of data breaches. *Infosec Institute*. https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches/

[40] Philippine News Agency. (2024, February 14). DICT probes possible hacking of DepEd office. https://www.pna.gov.ph/articles/1218862

[41] Philippine Star. (2024, December 9). PLM's Facebook page was hacked. *The Philippine Star*. https://www.philstar.com/nation/2024/12/09/2406046/plms-facebook-page-hacked

[42] Prümmer, J. (2024). Cybersecurity threats in educational institutions: Challenges and mitigation strategies. https://www.researchgate.net/publication/376000000_Cybersecurity_threats_in_educational_institutions

[43] Pugong, F. J. A. (2025). Assessing information security awareness for a tailored intervention program: A study of employees at Ifugao State University. *Journal of Arts, Humanities and Social Science*, 2(3), 143-155. https://journals.stecab.com/jahss/article/view/1132

[44] Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778. https://doi.org/10.2307/25750704

[45] Robbins, S. P. & Judge, T. A. (2017). *Organizational behavior* (17th ed.). Pearson Education.

[46] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93-114. https://tinyurl.com/2hvku3y4

[47] Romblon State University. (2024, November). Bid bulletin: Clarification No. 3 — RSU-2024-10-088. https://rsu.edu.ph/wp-content/uploads/2024/11/Clarification-No.-3-RSU-2024-10-088.pdf

[48] Roy, R., & Francis, J. J. (2023). The impact of cybercrime awareness training among employees in corporations for better information management. *Academy of Marketing Studies Journal*, 27(S5), 1-6. https://tinyurl.com/46vhnw7c

[49] Sapanca, H. F. (2022). Risk management in digitalized educational environments. *Frontiers in Psychology*. https://doi.org/10.3389/fpsyg.2022.986561

[50] Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W. W. Norton & Company.

[51] Shillair, R. (2020). Protection motivation theory. In J. Bryant & P. Vorderer (Eds.), *The international encyclopedia of media psychology* (pp. 1-8). Wiley.

[52] Souppaya, M. & Scarfone, K. (2016). User's Guide to Telework and Bring Your Own Device (BYOD) Security (NIST SP 800-114). https://doi.org/10.6028/NIST.SP.800-114r1

[53] Taherdoost, H. (2024). Impact of employee cybersecurity awareness on security incidents. *Journal of Cybersecurity*.

[54] Tomas, D. L. D. (2024, September 12). University personnel trained on cybersecurity in DICT workshop. *Ifugao State University*. https://tinyurl.com/4hr38he4

[55] Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program (NIST SP 800-50). https://doi.org/10.6028/NIST.SP.800-50