

# From Awareness to Practice: Domain-Specific Information Security Awareness as a Predictor of Self-Reported Cybersecurity Practices among University Personnel

Noli B. Lucila Jr.

College of Science, Bicol University, Legazpi City, 4500, Philippines; nlucila@bicol-u.edu.ph

**Abstract:** This study examined information security awareness as a predictor of self-reported cybersecurity practices among 160 personnel of a state university in the Philippines. Awareness was measured across six domains: password security, phishing, device security, data protection, security policy, and social engineering. Results showed moderate to high awareness and reported practices, with uneven domain patterns. Multiple regression indicated that awareness domains explained 55.8% of the variance in reported practices. Password security, phishing, and social engineering awareness were significant predictors, while security policy, data protection, and device security were not. However, these findings should be understood in the context of self-reported cybersecurity practices, which may differ from actual behavior.

**Keywords:** information security awareness, cybersecurity practices, self-reported cybersecurity readiness, human factors in cybersecurity, higher education cybersecurity, security behavior

---

## 1 Introduction

Organizations across sectors increasingly depend on digital technologies to support communication, decision-making, record management, and service delivery. In higher education institutions, information systems manage student enrollment, academic records, research data, financial transactions, and organizational communication. While interconnected platforms improve efficiency and accessibility, they also increase exposure to cybersecurity threats. In fact, universities store large volumes of sensitive information while maintaining relatively open network environments to support teaching and research collaboration, making them frequent targets of cyberattacks [1].

Traditional cybersecurity strategies have primarily emphasized technological safeguards such as encryption, intrusion detection systems, and access control mechanisms. Although these controls remain essential, security incidents continue to occur despite increasingly sophisticated protections. Evidence consistently indicates that human actions contribute significantly to cybersecurity breaches, including responding to phishing emails, mishandling confidential data, sharing credentials, or neglecting software updates [2]. These findings highlight a fundamental limitation of technology-centered approaches: organizational protection depends not only on technical infrastructure but also on the behavior of users interacting with information systems. Consequently, cybersecurity is increasingly recognized as a socio-technical challenge requiring both technological controls and human-centered interventions [3].

Growing recognition of the human role in cybersecurity incidents has led to increased interest in information security awareness, defined as individuals' understanding of security risks, organizational policies, and appropriate protective actions when interacting with information systems [4]. Organizations commonly implement awareness programs to educate personnel about safe practices such as identifying

suspicious communications, protecting credentials, securing devices, and safeguarding institutional data. However, empirical evidence suggests that awareness does not automatically translate into secure practice. Users frequently exhibit a gap between knowledge and behavior, often described as the knowing-doing gap in cybersecurity. Individuals may recognize phishing characteristics yet still respond to malicious messages due to urgency, routine habits, or perceived convenience [5]. These patterns indicate that awareness alone does not guarantee organizational protection.

Recent research therefore distinguishes awareness from cybersecurity readiness. Awareness represents cognitive understanding of threats and policies, whereas cybersecurity readiness reflects preparedness to apply protective actions consistently in real-world situations. Behavioral security frameworks such as the Human Aspects of Information Security Questionnaire (HAIS-Q) conceptualize information security awareness as a multidimensional construct involving knowledge, attitudes, and behavior [6]. This perspective is important because it emphasizes that cybersecurity awareness should not be treated merely as factual knowledge, but as a behavioral construct connected to actual or reported security practices.

However, in survey-based studies, readiness is often operationalized through reported cybersecurity practices rather than directly observed behavior. In the present study, cybersecurity readiness is therefore interpreted cautiously as self-reported behavioral readiness, measured through respondents' reported cybersecurity practices. This distinction is important because self-reported practices may reflect perceived, intended, or socially desirable behavior and may not fully capture actual technical actions, such as responses to simulated phishing attempts, system log events, incident-reporting records, or observed responses to social engineering scenarios.

Building from HAIS-Q and related human-centered cybersecurity perspectives, this study does not claim to introduce an entirely new theory of awareness. Rather, it applies and extends the behavioral logic of existing awareness frameworks by examining how specific awareness domains are associated with self-reported cybersecurity practices in a higher education context. This domain-specific approach is important because different types of awareness may not translate into cybersecurity practices with equal strength. For instance, awareness domains related to everyday security decisions, such as password security, phishing detection, and social engineering recognition, may be more closely associated with reported practices than more procedural domains such as policy awareness or data protection awareness.

Furthermore, this behavioral perspective is particularly relevant in higher education environments. Universities operate decentralized and collaborative infrastructures where strict technical restrictions may hinder academic activities. Faculty and administrative personnel must independently interpret policies, manage digital resources, and evaluate potential threats [7]. Because enforcement mechanisms are often limited, organizational protection relies heavily on voluntary compliance with security practices. Consequently, cybersecurity posture reflects collective cybersecurity readiness shaped by both awareness and the routine security behaviors that personnel report applying in their daily work.

Moreover, information security awareness is multidimensional and spans domains such as password management, phishing detection, device security, data protection, policy compliance, and social engineering awareness. Each domain represents a layer of human defense against cyber threats, and attackers often exploit the weakest behavioral layer [8]. Evaluating awareness across domains therefore provides deeper insight into areas of strength and vulnerability in organizational cybersecurity readiness. Unlike prior studies that rely primarily on descriptive awareness indicators, this study empirically models information security awareness as a predictor of self-reported cybersecurity practices.

Therefore, this study examines information security awareness as a predictor of self-reported cybersecurity practices among university personnel. Specifically, it addresses the following research questions: (RQ1) What are the levels of information security awareness and self-reported cybersecurity practices across domains? (RQ2) Which domains demonstrate strengths and vulnerabilities in cybersecurity readiness? and (RQ3) To what extent does information security awareness predict self-reported cybersecurity practices? By interpreting awareness as a multidimensional behavioral defense capability rather than a descriptive measure of knowledge alone, this study contributes to human-centered cybersecurity research and provides guidance for designing more targeted organizational cybersecurity awareness programs.

## 2 Review of Related Literature

### 2.1 *Information Security Awareness*

Information security awareness has been widely recognized as a fundamental component of organizational cybersecurity. It refers to the extent to which individuals understand organizational policies, recognize potential threats, and know appropriate protective actions when interacting with information systems [4]. Early research conceptualized information security awareness primarily as a process of knowledge acquisition. Organizations therefore implemented awareness programs focused on educating users about password safety, email threats, and acceptable use policies under the assumption that informed users would naturally behave securely.

Subsequent research, however, identified persistent gaps between knowledge and behavior. For instance, [9] demonstrated that awareness campaigns may improve understanding but do not consistently improve compliance unless supported by behavioral reinforcement mechanisms. Employees who can explain security policies may still fail to follow them in practice, indicating that awareness alone does not guarantee organizational protection. These findings suggest that knowledge-based awareness programs may be insufficient without mechanisms that encourage behavioral adoption.

In addition, the Human Aspects of Information Security Questionnaire (HAIS-Q) framework further clarifies this distinction by conceptualizing information security awareness as a multidimensional construct consisting of knowledge, attitude, and behavior components [6]. Knowledge represents cognitive understanding of security rules, attitude reflects the perceived importance of security, and behavior involves the performance of protective actions. From this perspective, awareness assessment should consider not only what users know but also how awareness is connected to security-related attitudes and behaviors.

The present study builds from this behavioral understanding of awareness. However, it does not claim to replace existing awareness frameworks such as HAIS-Q. Rather, it applies the behavioral logic of human-centered cybersecurity models by examining how specific awareness domains are associated with self-reported cybersecurity practices among university personnel. This domain-level focus is important because different forms of awareness may not translate into cybersecurity practices with equal strength.

### 2.2 *Human Factors and Cybersecurity Behavior*

Cybersecurity incidents frequently originate from human interaction rather than technical failure. For example, social engineering attacks exploit psychological tendencies such as trust, urgency, and authority, enabling attackers to bypass technical defenses [10]. As a matter of fact, large-scale breach analyses consistently identify user behavior as a major contributing factor in successful attacks [2]. These findings have shifted cybersecurity research toward understanding behavioral vulnerabilities rather than focusing solely on technological defenses.

Research literature indicates that users often make trade-offs between convenience and security. [11] argued that individuals may disregard security recommendations when the perceived effort outweighs the expected benefits. For example, complex password requirements may encourage password reuse across systems, while security mechanisms such as multi-factor authentication may be bypassed when perceived as inconvenient. These behaviors may occur even among knowledgeable users, reinforcing the conclusion that awareness alone does not automatically produce secure practice.

Furthermore, organizational context shapes security behavior. [12] found that policy compliance increases when users perceive security procedures as relevant and fair. Conversely, impractical or overly restrictive procedures may encourage workarounds that undermine organizational protection. Security behavior therefore emerges from the interaction between individual cognition and organizational environment, supporting the view of cybersecurity as a socio-technical phenomenon rather than solely a technical or educational outcome.

### 2.3 *Awareness as Behavioral Readiness*

Recent literature increasingly distinguishes information security awareness from cybersecurity readiness. Awareness refers to understanding threats and procedures, whereas readiness reflects preparedness to apply protective actions consistently in real situations [13]. Readiness develops when secure behavior becomes habitual and embedded in everyday routines. Users who instinctively verify suspicious messages, protect credentials, update devices, and avoid risky online actions demonstrate readiness rather than mere

awareness. Information security awareness spans multiple behavioral domains, including password management, email handling, device security, data protection, and incident response. Each domain represents a layer of human defense against cyber threats. Attackers typically exploit the weakest behavioral layer rather than attempting to bypass all safeguards simultaneously [14]. Evaluating awareness across domains therefore provides insight into organizational resilience and cybersecurity readiness.

Moreover, behavioral maturity develops progressively. Individuals initially learn rules, form attitudes toward them, and eventually develop habits through repetition [9]. Habit formation is critical because secure behavior must occur automatically under time pressure or cognitive load. Consequently, awareness measurement should focus on readiness across domains rather than isolated knowledge scores.

In the present study, however, cybersecurity readiness is operationalized through self-reported cybersecurity practices. This means that readiness is interpreted as reported behavioral readiness rather than objectively verified cybersecurity behavior. Self-reported measures are useful for assessing how personnel perceive and report their security practices, but they may also be affected by social desirability bias, recall limitations, or institutional expectations. Thus, the study treats reported cybersecurity practices as indicators of readiness while recognizing that actual behavior would require additional validation through simulated phishing exercises, system logs, incident reports, or direct observation.

## 2.4 *Cybersecurity Awareness in Higher Education*

Higher education institutions present unique cybersecurity challenges due to openness, diversity of users, and decentralized technology environments. Universities encourage collaboration and information sharing, often allowing broad network access across multiple devices. While such openness supports academic activities, it also increases exposure to cyber threats and complicates enforcement of strict technical controls [7]. Additionally, personnel in universities perform varied roles and possess differing levels of technical expertise. Administrative staff, faculty members, and support personnel interact with organizational systems differently, leading to variation in cybersecurity behavior. Because universities cannot impose highly restrictive controls without affecting academic freedom, organizational protection depends heavily on voluntary compliance with security practices [15].

Empirical studies show uneven awareness patterns within academic communities. Personnel commonly demonstrate adequate understanding of password practices but weaker readiness in reporting incidents and managing sensitive data [9]. Attackers frequently exploit these behavioral gaps through phishing attacks and credential harvesting. Organizational security posture therefore depends on strengthening readiness across multiple domains rather than focusing on isolated security practices. Universities also face challenges related to decentralized technology use. Personal devices, external platforms, and remote access increase reliance on individual decision-making. Users must frequently interpret security cues independently, reinforcing the importance of behavioral readiness rather than simple awareness. These conditions make higher education an important context for examining how information security awareness is associated with cybersecurity practices.

## 2.5 *Research Gap*

Existing literature widely acknowledges the importance of information security awareness but frequently evaluates awareness using descriptive indicators such as average awareness scores. Many organizational assessments measure awareness levels without examining how awareness patterns translate into cybersecurity readiness or how domain-specific awareness contributes to consistent security practices. Consequently, organizations may overestimate their cybersecurity readiness despite vulnerabilities within specific behavioral domains.

Although the HAIS-Q framework already conceptualizes awareness through knowledge, attitude, and behavior [6], additional empirical work is needed to examine how specific awareness domains relate to cybersecurity practices in particular institutional contexts. In higher education institutions, this issue is especially important because personnel operate within open, decentralized, and collaborative environments where technical restrictions may be limited and voluntary compliance becomes essential.

In addition, few studies have empirically examined information security awareness as a domain-specific predictor of self-reported cybersecurity practices among university personnel. In particular, limited research has investigated whether behavior-oriented awareness domains, such as password security, phishing detection, and social engineering awareness, are more strongly associated with cybersecurity practices than policy-oriented domains, such as security policy awareness and data protection awareness.

This study addresses these limitations by examining information security awareness as a multidimensional predictor of self-reported cybersecurity practices among university personnel. By analyzing domain-level awareness patterns and their relationships with reported cybersecurity practices, the study interprets security awareness as a human defense capability while cautiously recognizing that self-reported practices are indicators of perceived behavioral readiness rather than direct measures of actual cybersecurity behavior. In doing so, the research contributes to human-centered cybersecurity studies by providing contextual evidence on how awareness domains are associated with cybersecurity practices in a higher education setting.

## 2.6 Conceptual Framework of the Study

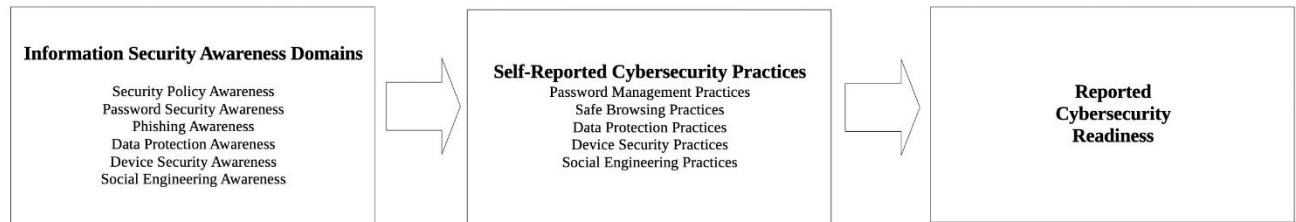
This study is grounded in human-centered cybersecurity and behavioral information security perspectives, particularly the view that information security awareness involves more than knowledge of threats and policies. Existing awareness frameworks, such as the HAIS-Q, conceptualize awareness as a multidimensional construct involving knowledge, attitudes, and behavior [6]. Building from this perspective, the present study examines how domain-specific information security awareness is associated with cybersecurity practices among university personnel.

The framework, as shown in Figure 1, does not claim to replace existing behavioral awareness models. Rather, it applies and contextualizes their logic within a higher education setting by examining awareness as a multidimensional antecedent of self-reported cybersecurity practices. In this study, information security awareness is represented by six domains: password security awareness, phishing awareness, device security awareness, data protection awareness, security policy awareness, and social engineering awareness. These domains reflect different areas of cybersecurity knowledge and judgment that may influence how personnel respond to routine security demands.

Cybersecurity practices serve as the outcome variable and are used as self-reported indicators of cybersecurity readiness. These practices include reported behaviors related to password management, phishing and email handling, device security, safe browsing, data protection, and social engineering response. Because these practices were measured through survey responses, the framework interprets readiness as reported behavioral readiness rather than objectively verified cybersecurity behavior.

Furthermore, the proposed framework assumes that awareness contributes to cybersecurity readiness when personnel translate knowledge of threats, policies, and protective actions into routine security practices. However, the framework also recognizes that awareness domains may not influence practices equally. Awareness domains directly connected to everyday security decisions, such as password security, phishing detection, and social engineering recognition, may be more strongly associated with reported cybersecurity practices than more procedural domains such as policy awareness or data protection awareness.

Thus, the framework positions information security awareness as a multidimensional behavioral antecedent, cybersecurity practices as self-reported manifestations of readiness, and overall cybersecurity readiness as an institutional condition reflected through the reported consistency of protective behaviors. This domain-differentiated approach allows the study to identify which awareness areas are more closely associated with cybersecurity practices and which areas may require further institutional support, training, or behavioral reinforcement.



**Figure 1.** Conceptual Framework of Information Security Awareness and Self-Reported Cybersecurity Practices

## 3 Methods

### 3.1 Research Design

This study employed a quantitative cross-sectional correlational research design to examine the

relationship between information security awareness and self-reported cybersecurity practices among university personnel. The design was appropriate because the study aimed to determine whether overall and domain-specific awareness were significantly associated with reported cybersecurity practices without manipulating the study variables. The study conceptualized information security awareness as a multidimensional behavioral antecedent of cybersecurity practices. Cybersecurity practices were used as self-reported indicators of cybersecurity readiness. Thus, readiness in this study refers to reported behavioral readiness rather than objectively verified cybersecurity performance. This distinction is important because the study measured respondents' reported practices through a survey and did not include objective behavioral measures such as simulated phishing exercises, system log analysis, incident-reporting records, or direct observation. Moreover, the cross-sectional design allowed the collection of data at one point in time and provided a snapshot of cybersecurity awareness and reported practices within the institution. However, because the data were cross-sectional, the study examined predictive associations rather than causal relationships.

### *3.2 Participants*

The participants consisted of 160 personnel from a state university in the Philippines. Respondents included faculty members, administrative personnel, technical staff, and support personnel who regularly interacted with institutional information systems in the performance of their duties. These personnel were considered appropriate respondents because they represent end users who handle institutional data, access digital platforms, communicate through online systems, and participate in routine cybersecurity-related behaviors.

Participation in the study was voluntary, and responses were collected anonymously to encourage honest reporting of cybersecurity awareness and practices. No personally identifiable information was collected. The sample size was considered sufficient for the correlational and regression analyses conducted in the study. However, because the participants came from a single institution, the findings should be interpreted as context-specific and should not be generalized to all higher education institutions without caution.

### *3.3 Research Instrument*

Data were collected using a structured questionnaire designed to measure information security awareness and cybersecurity practices across multiple domains. The instrument was informed by established information security awareness literature and human-centered cybersecurity perspectives, including the view that awareness involves knowledge, attitudes, and behavior [6].

The questionnaire consisted of two major components. The first component measured information security awareness across six domains: password security awareness, phishing awareness, device security awareness, data protection awareness, security policy awareness, and social engineering awareness. These domains assessed respondents' understanding of common cybersecurity threats, organizational security expectations, and appropriate protective actions. The second component measured cybersecurity practices as self-reported indicators of behavioral readiness. The practice domains included password management practices, phishing and email handling practices, device security practices, safe browsing practices, data protection practices, and social engineering practices. These domains assessed the extent to which respondents reported applying protective cybersecurity behaviors in their routine work activities.

All items were measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). Higher scores indicated stronger information security awareness or more consistent reported implementation of cybersecurity practices. Composite scores were computed by averaging the items corresponding to each awareness and practice domain. Overall information security awareness was computed by averaging the awareness domain scores, while overall cybersecurity practices were computed by averaging the practice domain scores. Because cybersecurity practices were self-reported, the resulting scores should be interpreted as perceived or reported behavioral readiness rather than direct evidence of actual cybersecurity behavior. This operational definition was adopted to align the statistical analysis with the survey-based nature of the data.

### *3.4 Data Collection Procedure*

Data were collected through a self-administered electronic survey distributed to university personnel. The online format was used to facilitate participation and ensure efficient data gathering. Respondents

completed the questionnaire individually and voluntarily. Before answering the survey, participants were informed of the purpose of the study, the voluntary nature of participation, and the anonymous treatment of responses. Completed responses were screened for completeness and consistency before analysis. Incomplete questionnaires were excluded from the dataset. Only valid responses were included in the final analysis. The final dataset consisted of 160 responses.

### 3.5 Data Analysis

Data analysis was conducted using Jamovi [16,17]. Descriptive statistics, including means and standard deviations, were used to summarize the levels of information security awareness and self-reported cybersecurity practices across domains. Cronbach's alpha was used to assess the internal consistency of the awareness and practice scales.

Similarly, Pearson correlation analysis was conducted to examine relationships among awareness domains and among cybersecurity practice domains. In addition, simple linear regression was used to determine whether overall information security awareness significantly predicted composite self-reported cybersecurity practices. Multiple regression analysis was then conducted to examine which specific awareness domains significantly predicted overall cybersecurity practices.

For the multiple regression model, the awareness domains were entered as predictor variables, while composite self-reported cybersecurity practices served as the outcome variable. The regression analysis reported unstandardized coefficients, standard errors, standardized beta coefficients, t-values, p-values, and confidence intervals. Multicollinearity diagnostics, including tolerance and variance inflation factor (VIF), were also reported to assess whether the awareness domains were excessively correlated. Statistical significance was evaluated at the 0.05 level.

## 4 Results

### 4.1 Reliability Analysis

The internal consistency of the measurement scales was assessed using Cronbach's alpha. The results indicated acceptable to excellent reliability across the information security awareness and cybersecurity practice constructs. For the awareness domains, Cronbach's alpha values ranged from 0.783 to 0.922. Specifically, phishing awareness obtained the highest reliability coefficient ( $\alpha = 0.922$ ), followed by security policy awareness ( $\alpha = 0.895$ ), data protection awareness ( $\alpha = 0.890$ ), social engineering awareness ( $\alpha = 0.897$ ), device security awareness ( $\alpha = 0.865$ ), and password security awareness ( $\alpha = 0.783$ ). All coefficients exceeded the commonly accepted threshold of 0.70, indicating satisfactory internal consistency.

The cybersecurity practice domains also demonstrated acceptable to excellent reliability. Data protection practices obtained the highest reliability coefficient ( $\alpha = 0.922$ ), followed by safe browsing practices ( $\alpha = 0.888$ ), social engineering practices ( $\alpha = 0.886$ ), device security practices ( $\alpha = 0.867$ ), and password management practices ( $\alpha = 0.791$ ). These results suggest that the survey items consistently measured their respective constructs and support the use of composite scores in the subsequent descriptive, correlation, and regression analyses.

However, the reliability results should be interpreted together with the study's operationalization of cybersecurity practices. Since the practice domains were measured through self-reported survey responses, the reliability coefficients indicate consistency of responses within each domain but do not validate actual cybersecurity behavior. Thus, the practice scores are treated as indicators of reported behavioral readiness rather than direct measures of observed cybersecurity performance.

### 4.2 Descriptive Statistics

#### 4.2.1 Information Security Awareness

Table 1 presents the descriptive statistics for the information security awareness domains among university personnel. Overall, respondents demonstrated moderate to high levels of information security awareness, indicating general familiarity with cybersecurity risks and protective procedures.

Password security awareness obtained the highest mean score ( $M = 4.18$ ,  $SD = 0.546$ ), suggesting that respondents had strong awareness of password-related security principles and practices. Device security

awareness also showed a relatively high mean score ( $M = 3.86$ ,  $SD = 0.674$ ), indicating familiarity with device protection measures. Phishing awareness obtained a moderate to high mean score ( $M = 3.69$ ,  $SD = 0.834$ ), although its relatively higher standard deviation suggests variation in respondents' ability to recognize phishing-related threats.

Data protection awareness ( $M = 3.52$ ,  $SD = 0.794$ ) and security policy awareness ( $M = 3.45$ ,  $SD = 0.773$ ) were lower than the more routine security domains, suggesting that knowledge of institutional data handling expectations and formal security policies may be less uniformly developed. Social engineering awareness obtained the lowest mean score ( $M = 3.33$ ,  $SD = 0.825$ ), indicating comparatively weaker awareness of manipulation-based and human-centered cybersecurity threats.

These findings suggest that personnel awareness is stronger in familiar and frequently emphasized areas such as password and device security, but weaker in more complex or less visible areas such as social engineering, policy awareness, and data protection. This uneven pattern indicates that cybersecurity awareness is multidimensional and that institutional training should not rely solely on general awareness campaigns.

**Table 1.** Descriptive Statistics for Information Security Awareness Domains

| Awareness Domain             | Mean | SD    | Minimum | Maximum |
|------------------------------|------|-------|---------|---------|
| Security Policy Awareness    | 3.45 | 0.773 | 1.40    | 5.00    |
| Password Security Awareness  | 4.18 | 0.546 | 3.00    | 5.00    |
| Phishing Awareness           | 3.69 | 0.834 | 1.00    | 5.00    |
| Data Protection Awareness    | 3.52 | 0.794 | 1.00    | 5.00    |
| Device Security Awareness    | 3.86 | 0.674 | 1.60    | 5.00    |
| Social Engineering Awareness | 3.33 | 0.825 | 1.20    | 5.00    |

Note.  $N = 160$ . Higher scores indicate stronger information security awareness. Values are based on a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree.

#### 4.2.2. Self-Reported Cybersecurity Practices

Table 2 presents the descriptive statistics for cybersecurity practice domains. These practice scores represent self-reported cybersecurity behaviors and are interpreted in this study as indicators of reported behavioral readiness.

**Table 2.** Descriptive Statistics for Self-Reported Cybersecurity Practice Domains

| Cybersecurity Practice Domain | Mean | SD    | Minimum | Maximum |
|-------------------------------|------|-------|---------|---------|
| Password Management Practices | 3.76 | 0.729 | 1.80    | 5.00    |
| Safe Browsing Practices       | 3.92 | 0.863 | 1.40    | 5.00    |
| Data Protection Practices     | 2.90 | 1.003 | 1.00    | 4.80    |
| Device Security Practices     | 3.63 | 0.888 | 1.80    | 5.00    |
| Social Engineering Practices  | 4.15 | 0.791 | 1.40    | 5.00    |

Note.  $N = 160$ . Higher scores indicate more consistent self-reported implementation of cybersecurity practices. Values are based on a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree.

Social engineering practices obtained the highest mean score ( $M = 4.15$ ,  $SD = 0.791$ ), followed by safe browsing practices ( $M = 3.92$ ,  $SD = 0.863$ ), password management practices ( $M = 3.76$ ,  $SD = 0.729$ ), and device security practices ( $M = 3.63$ ,  $SD = 0.888$ ). These results suggest that respondents generally reported applying protective behaviors in routine cybersecurity situations, particularly in responding cautiously to suspicious communications and practicing safe online behavior.

Data protection practices obtained the lowest mean score ( $M = 2.90$ ,  $SD = 1.003$ ), indicating a comparatively weak area of reported cybersecurity behavior. The higher standard deviation also suggests greater variability in how respondents reported managing, storing, sharing, and protecting institutional data. This finding points to data protection as a potential vulnerability in the institution's reported cybersecurity readiness.

However, one notable descriptive pattern warrants careful interpretation: the divergence between social engineering awareness and social engineering practices. Social engineering awareness obtained the lowest

mean score among the awareness domains, whereas social engineering practices obtained the highest mean score among the practice domains. This pattern should not be interpreted to mean that respondents possess limited conceptual understanding of social engineering threats yet demonstrate objectively superior protection against such attacks. Rather, the divergence may be attributable to differences in the constructs captured by the two measures. The awareness items may have assessed respondents' conceptual familiarity with social engineering tactics, such as manipulation, impersonation, urgency cues, and deceptive requests, whereas the practice items may have captured broader self-reported cautious behaviors, such as avoiding suspicious links, declining unusual requests, or verifying messages before responding.

This finding may also be influenced by response-related and institutional factors. Because the practice measures were self-reported, respondents may have overstated desirable security behaviors due to social desirability bias or perceived institutional expectations. In addition, institutional controls such as email filtering mechanisms, automated security warnings, and periodic security reminders may have supported protective behavior even when conceptual awareness of social engineering remained comparatively limited. Accordingly, the high mean score for social engineering practices should be interpreted as reported protective behavior rather than verified resistance to actual social engineering attacks. This reinforces the need to treat cybersecurity practices in the present study as self-reported indicators of behavioral readiness rather than direct measures of observed cybersecurity performance.

### 4.3 *Correlation Analysis*

Pearson correlation analysis was conducted to examine the relationships among the information security awareness domains and among the self-reported cybersecurity practice domains. The analysis was performed to determine whether the domains within each construct were statistically related and whether they reflected coherent but distinct dimensions of awareness and practice.

#### 4.3.1. Information Security Awareness Domains

Table 3 presents the correlation matrix for the information security awareness domains. The results showed that all awareness domains were positively and significantly correlated with one another at  $p < 0.001$ . This indicates that respondents who reported higher awareness in one cybersecurity area also tended to report higher awareness in other areas.

The strength of the correlations ranged from moderate to strong, with coefficients ranging from  $r = 0.451$  to  $r = 0.814$ . These findings suggest that the awareness domains are interconnected components of a broader information security awareness construct. Personnel who are more aware of one cybersecurity domain are generally more likely to be aware of other related domains.

The strongest relationship was observed between data protection awareness and device security awareness ( $r = 0.814, p < 0.001$ ). This suggests that respondents who reported stronger understanding of data protection principles also tended to report stronger awareness of device security risks. Strong correlations were also observed between phishing awareness and data protection awareness ( $r = 0.774, p < 0.001$ ), phishing awareness and device security awareness ( $r = 0.762, p < 0.001$ ), and phishing awareness and social engineering awareness ( $r = 0.721, p < 0.001$ ). These relationships indicate that awareness of email-based and manipulation-based threats is closely associated with broader cybersecurity understanding.

**Table 3.** Pearson Correlation Matrix for Information Security Awareness Domains

| Variable                        | 1        | 2        | 3        | 4        | 5        | 6 |
|---------------------------------|----------|----------|----------|----------|----------|---|
| 1. Security Policy Awareness    | -        |          |          |          |          |   |
| 2. Password Security Awareness  | 0.509*** | -        |          |          |          |   |
| 3. Phishing Awareness           | 0.451*** | 0.593*** | -        |          |          |   |
| 4. Data Protection Awareness    | 0.596*** | 0.723*** | 0.774*** | -        |          |   |
| 5. Device Security Awareness    | 0.507*** | 0.678*** | 0.762*** | 0.814*** | -        |   |
| 6. Social Engineering Awareness | 0.466*** | 0.509*** | 0.721*** | 0.696*** | 0.699*** | - |

Note. N = 160. \*\*\* $p < 0.001$ .

Security policy awareness demonstrated comparatively weaker, although still significant, correlations with other awareness domains ( $r = 0.451$  to  $r = 0.596$ ,  $p < 0.001$ ). This pattern suggests that awareness of institutional policies may represent a more formal or procedural dimension of cybersecurity awareness, while domains such as phishing, device security, data protection, and social engineering may be more closely connected to everyday threat recognition and practical decision-making.

Across the findings, the significant positive correlations support the interpretation of information security awareness as a multidimensional but coherent construct. However, the presence of several strong correlations also indicates the need to assess multicollinearity in the regression analysis. Therefore, tolerance and variance inflation factor values should be reported in the multiple regression model to determine whether the awareness domains can be interpreted as distinct predictors of self-reported cybersecurity practices.

#### 4.3.2. Self-Reported Cybersecurity Practice Domains

Pearson correlation analysis was conducted to examine the relationships among the self-reported cybersecurity practice domains. As shown in Table 4, all practice domains were positively and significantly correlated at  $p < 0.001$ . The correlation coefficients ranged from moderate to strong, with values ranging from  $r = 0.532$  to  $r = 0.766$ . These findings indicate that respondents who reported stronger cybersecurity practices in one domain also tended to report stronger practices in other domains.

The strongest correlation was observed between Safe Browsing Practices and Device Security Practices ( $r = 0.766$ ,  $p < 0.001$ ), suggesting that respondents who reported safer online behavior also tended to report stronger device protection practices. A strong relationship was also found between Safe Browsing Practices and Social Engineering Practices ( $r = 0.734$ ,  $p < 0.001$ ), indicating that reported caution in online environments is closely associated with reported caution toward suspicious messages, links, requests, or manipulation attempts.

Moderately strong correlations were also observed between Password Management Practices and Device Security Practices ( $r = 0.666$ ,  $p < 0.001$ ), Data Protection Practices and Device Security Practices ( $r = 0.694$ ,  $p < 0.001$ ), and Password Management Practices and Data Protection Practices ( $r = 0.648$ ,  $p < 0.001$ ). Overall, these findings suggest that the practice domains form an internally coherent set of reported cybersecurity behaviors. However, because these are self-reported practices, the results should be interpreted as associations among reported behaviors rather than evidence of objectively verified cybersecurity performance.

**Table 4.** Pearson Correlation Matrix for Self-Reported Cybersecurity Practice Domains

| Variable                         | 1        | 2        | 3        | 4        | 5 |
|----------------------------------|----------|----------|----------|----------|---|
| 1. Password Management Practices | -        |          |          |          |   |
| 2. Safe Browsing Practices       | 0.594*** | -        |          |          |   |
| 3. Data Protection Practices     | 0.648*** | 0.662*** | -        |          |   |
| 4. Device Security Practices     | 0.666*** | 0.766*** | 0.694*** | -        |   |
| 5. Social Engineering Practices  | 0.583*** | 0.734*** | 0.532*** | 0.579*** | - |

Note. N = 160. \*\*\* $p < 0.001$ .

#### 4.4 Regression Analysis

Regression analysis was conducted to examine the extent to which information security awareness predicts self-reported cybersecurity practices among university personnel. While the correlation analysis established significant relationships among the awareness and practice domains, regression analysis was used to determine the predictive contribution of overall awareness and domain-specific awareness to reported cybersecurity practices.

In interpreting the regression results, it is important to note that the outcome variable represents self-reported cybersecurity practices. Therefore, the findings indicate predictive associations with reported behavioral readiness rather than objectively verified cybersecurity performance. The results should not be interpreted as evidence that awareness directly causes actual secure behavior, since the study used a cross-sectional survey design and did not include objective behavioral measures such as simulated phishing responses, system logs, or observed incident-reporting behavior.

##### 4.4.1. Composite Information Security Awareness as a Predictor of Self-Reported Cybersecurity Practices

Simple linear regression was conducted to determine whether overall information security awareness significantly predicted composite self-reported cybersecurity practices. The results showed that overall information security awareness was a significant positive predictor of self-reported cybersecurity practices,  $B = 0.857$ ,  $SE = 0.0636$ ,  $\beta = 0.732$ ,  $t = 13.49$ ,  $p < 0.001$ , as shown in Table 5. The model explained 53.5% of the variance in overall reported cybersecurity practices,  $R = 0.732$ ,  $R^2 = 0.535$ . This indicates that personnel with higher levels of information security awareness tended to report more consistent cybersecurity practices. However, because the outcome variable was based on self-reported practices, the result should be interpreted as evidence of association with reported behavioral readiness rather than objectively verified cybersecurity behavior.

**Table 5.** Simple Linear Regression Predicting Self-Reported Cybersecurity Practices from Overall Information Security Awareness

| Predictor                              | B     | SE     | $\beta$ | t     | p       | 95% CI for B    | Tolerance | VIF  |
|----------------------------------------|-------|--------|---------|-------|---------|-----------------|-----------|------|
| Intercept                              | 0.524 | 0.2367 | -       | 2.21  | 0.028   | [0.0560, 0.991] | -         | -    |
| Overall Information Security Awareness | 0.857 | 0.0636 | 0.732   | 13.49 | < 0.001 | [0.7318, 0.983] | 1.00      | 1.00 |

Note. N = 160. B = unstandardized coefficient; SE = standard error;  $\beta$  = standardized coefficient; CI = confidence interval; VIF = variance inflation factor. Model fit:  $R = 0.732$ ,  $R^2 = 0.535$ .

##### 4.4.2. Awareness Domains as Predictors of Self-Reported Cybersecurity Practices

Multiple regression analysis was conducted to examine which information security awareness domains significantly predicted composite self-reported cybersecurity practices. The awareness domains were entered as predictor variables, while composite self-reported cybersecurity practices served as the outcome variable.

The model explained a substantial proportion of variance in self-reported cybersecurity practices,  $R = 0.747$ ,  $R^2 = 0.558$ , Adjusted  $R^2 = 0.541$ . This indicates that the six awareness domains collectively accounted for 55.8% of the variance in reported cybersecurity practices. The findings suggest that domain-specific

information security awareness is meaningfully associated with personnel's reported cybersecurity behavior.

**Table 6.** Multiple Regression Predicting Self-Reported Cybersecurity Practices from Information Security Awareness Domains

| Predictor                    | B       | SE     | $\beta$ | t      | p     | 95% CI for B     | Tolerance | VIF  |
|------------------------------|---------|--------|---------|--------|-------|------------------|-----------|------|
| Intercept                    | 0.3171  | 0.3242 | -       | 0.978  | 0.330 | [-0.3234, 0.958] | -         | -    |
| Security Policy Awareness    | 0.0702  | 0.0638 | 0.0749  | 1.100  | 0.273 | [-0.0559, 0.196] | 0.624     | 1.60 |
| Password Security Awareness  | 0.2646  | 0.1073 | 0.1992  | 2.466  | 0.015 | [0.0526, 0.477]  | 0.443     | 2.26 |
| Phishing Awareness           | 0.2408  | 0.0838 | 0.2772  | 2.874  | 0.005 | [0.0753, 0.406]  | 0.311     | 3.22 |
| Data Protection Awareness    | -0.0467 | 0.1053 | -0.0511 | -0.444 | 0.658 | [-0.2547, 0.161] | 0.217     | 4.60 |
| Social Engineering Awareness | 0.2374  | 0.0739 | 0.2701  | 3.213  | 0.002 | [0.0914, 0.383]  | 0.409     | 2.45 |
| Device Security Awareness    | 0.1275  | 0.1116 | 0.1185  | 1.142  | .0255 | [-0.0931, 0.348] | 0.268     | 3.73 |

Note. N = 160. B = unstandardized coefficient; SE = standard error;  $\beta$  = standardized coefficient; CI = confidence interval; VIF = variance inflation factor. Model fit: R = 0.747, R<sup>2</sup> = 0.558, Adjusted R<sup>2</sup> = 0.541.

Among the six predictors, password security awareness, phishing awareness, and social engineering awareness emerged as significant positive predictors of self-reported cybersecurity practices. Password security awareness significantly predicted reported cybersecurity practices, B = 0.2646, SE = 0.1073,  $\beta$  = 0.1992, t = 2.466,  $p$  = 0.015. Phishing awareness was also a significant positive predictor, B = 0.2408, SE = 0.0838,  $\beta$  = 0.2772, t = 2.874,  $p$  = 0.005. Social engineering awareness likewise significantly predicted reported cybersecurity practices, B = 0.2374, SE = 0.0739,  $\beta$  = 0.2701, t = 3.213,  $p$  = 0.002.

In contrast, security policy awareness, data protection awareness, and device security awareness were not significant predictors. Security policy awareness did not significantly predict reported practices, B = 0.0702, SE = 0.0638,  $\beta$  = 0.0749, t = 1.100,  $p$  = 0.273. Data protection awareness was also not significant, B = -0.0467, SE = 0.1053,  $\beta$  = -0.0511, t = -0.444,  $p$  = 0.658. Device security awareness did not significantly predict reported practices, B = 0.1275, SE = 0.1116,  $\beta$  = 0.1185, t = 1.142,  $p$  = 0.255.

The standardized coefficients indicate that phishing awareness had the strongest positive association with self-reported cybersecurity practices ( $\beta$  = 0.2772), followed closely by social engineering awareness ( $\beta$  = 0.2701), and password security awareness ( $\beta$  = 0.1992). This pattern suggests that awareness domains directly connected to everyday threat recognition and routine security decisions are more strongly associated with reported cybersecurity practices than procedural or infrastructure-oriented awareness domains.

Multicollinearity diagnostics were also examined because several awareness domains were moderately to strongly correlated. The tolerance values ranged from 0.217 to 0.624, while VIF values ranged from 1.60 to 4.60. These values indicate that multicollinearity was present at a moderate level but did not exceed the commonly used threshold of serious concern. Therefore, the predictors were retained in the model.

#### 4.5 Integrated Interpretation of Findings

The findings demonstrate that information security awareness is significantly associated with self-reported cybersecurity practices among university personnel. The descriptive results showed moderate to high levels of awareness and reported practices across most domains, while the correlation analysis indicated that both awareness and practice domains were positively and significantly interrelated. The regression results further showed that the six awareness domains collectively explained 55.8% of the variance in composite self-reported cybersecurity practices, indicating that information security awareness is an important predictor of reported behavioral readiness.

However, the results also show that awareness does not translate into reported cybersecurity practices uniformly across domains. Password security awareness, phishing awareness, and social engineering awareness significantly predicted composite self-reported cybersecurity practices. These domains are closely connected to everyday security decisions, such as managing credentials, identifying suspicious messages, and responding cautiously to manipulation attempts. In contrast, security policy awareness, data protection awareness, and device security awareness were not significant predictors. This suggests that more procedural or infrastructure-oriented awareness domains may not automatically lead to reported security behavior unless supported by practical reinforcement, institutional guidance, and routine application.

A key finding requiring careful interpretation is the apparent discrepancy between social engineering

awareness and social engineering practices. Social engineering awareness obtained the lowest mean among the awareness domains, while social engineering practices obtained the highest mean among the practice domains. This pattern does not necessarily indicate that respondents have weak conceptual knowledge of social engineering yet objectively demonstrate superior protective behavior. Rather, it may reflect differences in measurement. The awareness items may have captured conceptual understanding of social engineering tactics, while the practice items may have captured general self-reported caution, such as avoiding suspicious links, verifying unusual requests, or refusing to share credentials.

This discrepancy may also be influenced by social desirability bias, institutional security reminders, or technical controls such as spam filters and email security systems that help reduce exposure to risky messages. Therefore, the high score for social engineering practices should be interpreted as reported protective behavior rather than verified resistance to actual social engineering attacks. This reinforces the need to interpret cybersecurity practices in this study as self-reported indicators of behavioral readiness, not as direct measures of actual cybersecurity performance.

Collectively, the findings support a domain-differentiated interpretation of the awareness-to-practice relationship. Awareness matters, but its behavioral relevance depends on whether the domain is directly connected to routine security decisions and whether personnel have opportunities to apply the knowledge in everyday work. Thus, the results suggest that cybersecurity readiness in higher education requires not only awareness dissemination but also practice-oriented training, behavioral reinforcement, and institutional mechanisms that help personnel translate awareness into consistent secure behavior.

## 4.6 *Discussion by Research Questions*

### 4.6.1. RQ1: What are the levels of information security awareness and self-reported cybersecurity practices among university personnel?

The results indicate that university personnel demonstrated moderate to high levels of information security awareness and self-reported cybersecurity practices across most domains. Password security awareness obtained the highest mean score, suggesting that respondents were most familiar with password-related security principles. Device security and phishing awareness also showed relatively high levels, indicating general familiarity with common cybersecurity risks and protective measures.

However, the lower mean scores for security policy awareness, data protection awareness, and social engineering awareness suggest that awareness is not evenly developed across domains. These results imply that personnel may be more familiar with frequently emphasized security topics, such as password protection, than with more complex or less visible domains, such as policy interpretation, data protection responsibilities, and human manipulation tactics.

For cybersecurity practices, respondents reported relatively strong practices in social engineering response, safe browsing, and password management. However, data protection practices obtained the lowest mean score, indicating a possible vulnerability in the institution's reported cybersecurity readiness. This finding suggests that personnel may need additional practical training on secure data storage, sharing, handling, and protection.

### 4.6.2. RQ2: Which awareness and practice domains indicate strengths and vulnerabilities in cybersecurity readiness?

The results suggest that password security awareness, safe browsing practices, and reported social engineering practices represent areas of relative strength. These domains are associated with routine cybersecurity decisions that personnel commonly encounter in their daily work. The relatively high scores may reflect repeated institutional reminders, common exposure to password and email-related guidance, or greater familiarity with these security topics.

In contrast, data protection emerged as a key vulnerability. Although data protection awareness was moderate, data protection practices obtained the lowest mean score among the practice domains and did not significantly predict composite self-reported cybersecurity practices in the regression model. This suggests a possible gap between understanding data protection principles and applying them consistently in routine work. Personnel may know that data should be protected but may lack clear procedures, practical tools, or consistent reinforcement for secure data handling.

Similarly, security policy awareness also appeared as a weaker area. Its non-significant regression result

suggests that knowing institutional security policies may not be sufficient to influence reported cybersecurity practices. This may occur when policies are perceived as abstract, difficult to apply, or disconnected from everyday work routines. In higher education settings, where personnel often work across decentralized systems and flexible environments, policies must be translated into concrete behavioral guidance to become practically meaningful.

The social engineering result should be interpreted with caution. Although social engineering practices obtained the highest mean score and social engineering awareness significantly predicted overall practices, social engineering awareness also had the lowest descriptive mean. This indicates that respondents may report cautious behavior toward suspicious interactions even when their conceptual understanding of social engineering remains limited. Thus, social engineering should still be treated as a training priority rather than as a fully developed area of readiness.

#### 4.6.3. RQ3: To what extent does information security awareness predict self-reported cybersecurity practices?

The regression results indicate that information security awareness significantly predicts self-reported cybersecurity practices. The multiple regression model explained 55.8% of the variance in overall reported security practices, suggesting that awareness domains collectively play an important role in reported behavioral readiness.

Among the six awareness domains, phishing awareness had the strongest standardized effect, followed closely by social engineering awareness and password security awareness. These findings suggest that awareness domains involving immediate threat recognition and everyday security decisions are more strongly associated with reported cybersecurity practices. Personnel who are more aware of phishing tactics, manipulation attempts, and password security principles are more likely to report applying protective cybersecurity behaviors.

In contrast, security policy awareness, data protection awareness, and device security awareness were not significant predictors. These findings suggest that not all awareness domains have equal behavioral influence. Policy and data-related awareness may require stronger institutional reinforcement, clearer procedures, and hands-on practice before they translate into consistent cybersecurity behavior. Similarly, device security awareness may be influenced by technical controls, institutional device management, or variability in personnel responsibility for device maintenance.

These findings refine the conceptual understanding of information security awareness by showing that awareness is not a uniform predictor of reported cybersecurity practices. Instead, the relationship appears domain-specific. Behavior-oriented domains are more strongly associated with reported practices, while procedural or infrastructure-oriented domains may require additional organizational support to influence behavior. However, because the study used self-reported data, the results should be interpreted as evidence of associations with reported cybersecurity practices rather than objective proof of actual secure behavior.

## 5 Conclusion

This study examined the relationship between information security awareness and self-reported cybersecurity practices among university personnel. The findings showed that personnel generally demonstrated moderate to high levels of information security awareness and reported cybersecurity practices, suggesting a baseline level of behavioral cybersecurity preparedness within the institution. However, the results also revealed uneven development across domains, indicating that cybersecurity readiness cannot be fully understood through overall awareness scores alone.

The regression results showed that the six awareness domains collectively explained 55.8% of the variance in self-reported cybersecurity practices. This finding suggests that information security awareness is meaningfully associated with reported cybersecurity behavior among university personnel. However, because the study relied on self-reported survey data, the findings should be interpreted as evidence of associations between awareness and reported practices rather than proof of actual cybersecurity behavior.

The findings further demonstrated that not all awareness domains influenced reported cybersecurity practices equally. Password security awareness, phishing awareness, and social engineering awareness significantly predicted overall reported security practices. These domains are closely related to routine cybersecurity decisions and immediate threat recognition. In contrast, security policy awareness, data protection awareness, and device security awareness did not significantly predict reported practices. This pattern suggests that practical and behavior-oriented awareness domains may have stronger links to

cybersecurity practices than procedural or infrastructure-oriented knowledge.

The study also identified important areas of vulnerability. Data protection practices obtained the lowest mean score, indicating a need to strengthen personnel capacity in secure data handling, storage, sharing, and protection. In addition, the discrepancy between low social engineering awareness and high reported social engineering practices suggests that reported protective behavior should be interpreted cautiously. This pattern may reflect measurement differences, social desirability bias, institutional reminders, or technical controls rather than objectively verified resistance to social engineering attacks.

Across the findings, the study supports a domain-differentiated understanding of information security awareness and cybersecurity practices in higher education. Awareness contributes to reported cybersecurity readiness, but its influence depends on the type of awareness and its connection to routine work behavior. For higher education institutions, strengthening cybersecurity requires not only general awareness campaigns but also practical, scenario-based, and behavior-oriented interventions that help personnel translate awareness into consistent secure practices.

### *5.1 Theoretical Implications*

This study contributes to human-centered cybersecurity research by providing empirical evidence on how domain-specific information security awareness is associated with self-reported cybersecurity practices among university personnel. Rather than treating awareness as a single general construct, the findings show that awareness domains differ in their relationship with reported cybersecurity behavior. This supports the view that information security awareness is multidimensional and that its behavioral relevance depends on the type of awareness being developed.

The study is consistent with existing behavioral awareness frameworks, particularly the Human Aspects of Information Security Questionnaire (HAIS-Q), which conceptualizes information security awareness as involving knowledge, attitudes, and behavior. However, the present study does not claim to replace or duplicate HAIS-Q. Instead, it extends the behavioral logic of such frameworks by examining how specific awareness domains function as predictors of self-reported cybersecurity practices in a higher education context.

The findings suggest that behavior-oriented awareness domains, such as password security awareness, phishing awareness, and social engineering awareness, are more strongly associated with reported cybersecurity practices than procedural or infrastructure-oriented domains such as security policy awareness, data protection awareness, and device security awareness. This distinction contributes to cybersecurity theory by showing that awareness does not translate into practice uniformly. Awareness appears to have stronger behavioral relevance when it is directly connected to routine security decisions, immediate threat recognition, and everyday digital actions.

At the same time, the findings reinforce the need for caution in theorizing cybersecurity readiness from survey-based data. Since cybersecurity practices were measured through self-report, the study's theoretical contribution is limited to reported behavioral readiness rather than objectively verified cybersecurity behavior. Thus, the awareness-to-practice interpretation should be understood as a contextual refinement of existing human-centered cybersecurity models, not as a universal theory of actual cybersecurity performance.

### *5.2 Practical Implications*

The findings of this study provide several practical implications for higher education institutions seeking to strengthen personnel's behavioral cybersecurity readiness and reported cybersecurity practices. First, the results suggest that awareness programs should prioritize practical and behavior-oriented cybersecurity training. Awareness domains such as password security, phishing detection, and social engineering response demonstrated the strongest influence on cybersecurity practices. Training programs that emphasize realistic scenarios and hands-on activities may therefore be more effective than programs focused primarily on policy communication. Second, the consistently lower performance in data protection practices indicates a critical area for improvement. Institutions should strengthen training and support mechanisms related to secure data management, including proper storage, sharing, and protection of sensitive information. Improving data protection practices may strengthen personnel's reported behavioral cybersecurity readiness. Third, the findings indicate that security policy awareness alone is insufficient to ensure secure behavior. Institutions should complement policy communication with behavioral reinforcement strategies such as practical exercises, simulations, and periodic reminders to encourage consistent cybersecurity practices. Finally, the results highlight the importance of continuous awareness development across multiple security domains.

Balanced awareness and consistent security practices across domains are necessary to reduce behavioral vulnerabilities and improve reported cybersecurity practices and behavioral readiness. Although the study provides valuable insights into the relationship between security awareness and cybersecurity readiness, the findings are based on data from a single institution, which may limit the generalizability of the results to other organizational contexts.

### 5.3 *Limitations of the Study*

This study has several limitations. First, cybersecurity practices were measured through self-reported survey responses. Although self-reported practices provide useful insight into personnel's perceived behavioral readiness, they do not necessarily reflect actual cybersecurity behavior. Respondents may overreport secure practices due to social desirability bias, perceived institutional expectations, or limited awareness of their own risky behavior. The study did not include objective behavioral measures such as simulated phishing exercises, system log analysis, incident-reporting records, or direct observation. Second, the discrepancy between low social engineering awareness and high reported social engineering practices suggests a possible measurement limitation. The awareness items may have assessed conceptual understanding of social engineering tactics, while the practice items may have captured general caution or socially desirable responses. Therefore, the high score for social engineering practices should not be interpreted as verified resistance to actual social engineering attacks. Third, the study was conducted among 160 personnel from a single public higher education institution in the Philippines. Although the sample was sufficient for the statistical analyses conducted, the institutional scope limits the generalizability of the findings to other universities or organizational contexts. The results should therefore be interpreted as context-specific evidence rather than a universal model of cybersecurity readiness in higher education. Lastly, the study used a cross-sectional design, which limits causal interpretation. The regression results show predictive associations between information security awareness and self-reported cybersecurity practices, but they do not establish that awareness directly causes secure behavior. Future studies should use longitudinal, multi-institutional, and behaviorally validated designs to strengthen the evidence base.

### 5.4 *Suggestions for Future Research*

Future research may extend this study by examining organizational cybersecurity awareness and practices across multiple institutions to improve generalizability of the findings. Comparative studies involving different organizational contexts may provide deeper insights into how organizational environments influence cybersecurity readiness. Longitudinal studies may also provide valuable insight into how organizational cybersecurity awareness and practices develop over time, particularly following awareness training interventions. Such studies could help identify the most effective strategies for strengthening organizational cybersecurity readiness. Future research may also incorporate additional behavioral and organizational variables such as security culture, perceived risk, and organizational support in order to develop a more comprehensive understanding of the factors influencing cybersecurity readiness.

#### **Funding**

This research received no external funding.

#### **Conflict of Interest Statement**

The author declares no conflicts of interest.

#### **Data Availability Statement**

The data supporting the findings of this study are not publicly available due to privacy and ethical restrictions involving human participants. Aggregated data may be made available from the corresponding author upon reasonable request and subject to applicable institutional and ethical approval.

#### **Acknowledgment**

The author expresses sincere appreciation to the university personnel who participated in this study. The author also acknowledges the administrative support provided by the concerned offices during the coordination and conduct of data collection.

## Reference

1. EDUCAUSE. “Top 10 IT Issues, 2022: The Higher Education We Deserve”. Available at: <https://er.educause.edu/articles/2021/11/top-10-it-issues-2022-the-higher-education-we-deserve> (Accessed on date: 15 January 2026). EDUCAUSE Review.
2. Verizon. “Data breach investigations report”. Available at <https://www.verizon.com/business/resources/reports/dbir/> (Accessed on date: 15 January 2026).
3. S.S. Iyer & B. Raji. Cybersecurity culture and organizational resilience: A human-centered approach to digital risk management. *American Journal of Industrial and Business Management*, 15(5), 748–766, 2025.
4. M. Nieves, K. Dempsey & V.Y. Pillitteri. “An introduction to information security (NIST Special Publication 800-12 Rev. 1)”. National Institute of Standards and Technology. Available at: <https://csrc.nist.gov/pubs/sp/800/12/r1/final>. (Accessed on date: 15 January 2026).
5. C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, 133–144, 2009.
6. K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac & T. Zwaans. The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40–51, 2017.
7. M.S. Tsauri. Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall. *Journal of Applied Informatics and Computing*, 9(4), 1127–1136, 2025.
8. A.K. Gwenthure & F.S. Rahayu. Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review. International. *Journal of Serious Games*, 11(1), 83–99, 2024.
9. M. Bada, A.M. Sasse & J.R.C. Nurse. “Cyber security awareness campaigns: Why do they fail to change behaviour?” Available at: <https://arxiv.org/abs/1901.02672> (Accessed on date: 15 January 2026).
10. K. Khadka & A.B. Ullah. Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information*, 24(3), 119, 2025.
11. S. Oh, H. Baek, J.H. Huh, T. Kim, W. Jeon, I. Oakley & H. Kim. Understanding and improving user adoption and security awareness in password checkup services. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–32, 2025.
12. P. Ifinedo. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69–79, 2014.
13. K. Parsons, E. Young, M. Butavicius, A. McCormac, M. Pattinson & C. Jerram. The influence of organisational information security culture on cybersecurity decision making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117–129, 2015.
14. N.C. Edeh. Cybersecurity and human factors: A literature review. *Cybersecurity for Decision Makers* (pp. 45–56), 2023.
15. M. G. Ali, *Cybersecurity Governance and Policy Development in Higher Education Institutions: A Strategic Framework for Resilience and Compliance*, Education Resources Information Center (ERIC), Report ED675147, 2025. Available at: <https://eric.ed.gov/?id=ED675147> (Accessed on date: 15 January 2026).
16. The Jamovi Project, *jamovi*, Version 2.6, Jamovi.org, 2024. Available at: <https://jamovi.org>. (Accessed on date: 15 January 2026).
17. R Core Team. *R: A Language and Environment for Statistical Computing*, Version 4.4. R Foundation for Statistical Computing, 2024. Available at: <https://www.R-project.org/> (Accessed on date: 15 January 2026).

#### **Author Biographies**

**Dr. Noli B. Lucila Jr.** is an Associate Professor at Bicol University in Legazpi City, Philippines, where he has been teaching in Information Technology for 20 years, and is actively engaged in research, and extension services. He holds a Doctor in Information Technology from De La Salle University, Manila, with research interests centered on information security, ICT in education, digital transformation, and technology-enabled community development. Prior to his academic career, he served as a Security Engineer at Internet Security Systems Philippines, in Makati City, where he gained professional experience in IT security operations and security technologies. This industry background informs his academic and research work, particularly in examining cybersecurity not only as a technical concern but also as a human, behavioral, and organizational issue. At Bicol University, he teaches Information Assurance and Security courses. Beyond academia, he leads extension initiatives that promote safe cybersecurity practices among non-IT individuals across different industries and community sectors, including MSMEs, local government units, educational institutions, and community organizations. Through these initiatives, he advocates practical, inclusive, and behavior-oriented cybersecurity education that helps individuals and organizations use digital technologies more safely and responsibly.