Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10, 439-453
2025
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v9i10.10445

Cybersecurity attitudes in higher education institutions: A behavioural analysis of faculty and staff in the United Arab Emirates

Said Badreddine[1,2], Tariq Alwada'n[2], Mohammad Abdur Razzaque[2], Ala Al Kafri[2], Asem Omari[1], Azmi Alazzam[1], Hamsa Al Ammari[3*]
[1]Computer Information Systems, Higher Colleges of Technology, Abu Dhabi, Al Ain, UAE.
[2]School of Computing, Engineering & Digital Technologies, Teesside University, Middlesbrough TS1 3BX, UK.
[3]Advisor of the Chief Academic Officer, Higher Colleges of Technology, Central Services, Abu Dhabi, UAE; hsaleh@hct.ac.ae (H.A.A.).

Abstract: Cybersecurity in higher education institutions (HEIs) is increasingly recognized as a behavioral and organizational challenge, not solely a technical one. This study investigates the perceptions, awareness, and attitudes of faculty and staff in UAE HEIs toward cybersecurity policies and practices, with a focus on how institutional communication, policy frameworks, and cultural dynamics shape behaviors. Semi-structured interviews were conducted with academic and administrative staff, generating rich qualitative data that were analyzed thematically. The findings reveal three dominant themes. First, cybersecurity training and communication are often symbolic, generic, and disconnected from daily professional contexts, limiting their ability to enhance coping appraisal. Second, misalignment between policy and practice results in frustration and circumvention, as rigid protocols undermine perceived behavioral control and conflict with academic autonomy. Third, organizational culture and peer dynamics play a decisive role in shaping norms of compliance or non-compliance, with weak cultural embedding leaving security viewed as an IT department responsibility rather than a shared institutional value. These findings were integrated into a conceptual model grounded in Protection Motivation Theory (PMT), the Theory of Planned Behavior (TPB), and the COM-B framework. The model demonstrates how institutional mechanisms and cultural factors converge on employee attitudes, which in turn drive secure or insecure behaviors. The study advances theoretical understanding of cybersecurity as a behavioral phenomenon and offers practical recommendations for HEIs, including role-specific training, participatory policy design, and cultural embedding. By addressing attitudinal drivers, HEIs in the UAE can build more resilient cybersecurity cultures in increasingly complex threat landscapes.

Keywords: *Behavioural Analysis, Cybersecurity Attitudes, Higher Education Institutions, Information Security Culture, UAE.*

1. Introduction

Universities are increasingly exposed to sophisticated cyber threats due to open networks, heterogeneous user populations, and the proliferation of cloud and IoT services. Evidence from higher education shows recurrent risks spanning phishing, ransomware, data exfiltration, and service disruption, with mission-critical assets frequently implicated. Recent syntheses underline nine strategic risk clusters specific to universities and call for institution-wide responses that integrate policy, culture, and user behavior [1]. National guidance similarly documents sustained targeting of the UK research and education sector, urging HEIs to prioritize human-centred controls alongside technical baselines [2]. Complementary assessments of UK universities map attack timelines against the confidentiality, integrity, and availability triad, reinforcing the sector's systemic exposure [3].

History: Received: 18 August 2025; Revised: 19 September 2025; Accepted: 23 September 2025; Published: 9 October 2025
* Correspondence: hsaleh@hct.ac.ae

Within this landscape, employee attitudes, including risk appraisal, perceived control, and normative pressures, are pivotal determinants of secure or insecure practice. Systematic reviews show that Protection Motivation Theory (PMT) dominates explanatory models of cybersecurity behaviour, with growing application of the Theory of Planned Behaviour (TPB); both emphasise threat/coping appraisal and intention formation, while COM-B highlights capability, opportunity, and motivation as proximal drivers of action [4, 5]. Empirical studies further indicate that coping-appraisal constructs (self-efficacy, response efficacy) often outweigh fear appeals in predicting compliance, underscoring the importance of cultivating positive security attitudes rather than relying on deterrence alone [6]. In academic settings, awareness and training frameworks are proposed to embed a security culture; yet most interventions remain student-centric, with fewer studies interrogating faculty and staff attitudes, the very groups who enact and interpret institutional policy [7].

1.1. Problem Statement

Despite maturing policy frameworks in the Gulf and sustained digital transformation across UAE higher education, there is limited qualitative evidence on how faculty and staff perceive cybersecurity policies and how those attitudes translate into everyday practice. This gap constrains human-centred policy design and behaviour-change strategies. Addressing it requires a behavioural analysis grounded in PMT, TPB, and COM-B to surface how attitudes, organisational culture, and perceived capability/opportunity shape secure conduct. This article responds by exploring cybersecurity attitudes among UAE HEI employees through semi-structured interviews, generating empirically grounded implications for policy communication, training, and cultural enablement.

1.2. Literature Review

1.2.1. Cyber Risk in Higher Education: Scope and Distinctives

Universities face a persistent concentration of cyber risks due to open networks, heterogeneous user groups, and valuable data assets (research IP, student records, and high-performance computing). A systematic review by Ulven and Wangen synthesized sector-specific threats (phishing, ransomware, abuse of institutional compute as attack staging) and mapped assets–threats–vulnerabilities in HEIs, arguing that technical controls are necessary but insufficient without governance and user-centric measures [1]. MDPI reviews focused on the UK university sector further show escalating incident timelines, with attacks classified across the confidentiality–integrity–availability triad and highlighting weaknesses in identity management and legacy systems [3]. The timeline in Figure 1 highlights the escalating scale and sophistication of cyberattacks targeting UK universities, illustrating systemic vulnerabilities across confidentiality, integrity, and availability. Incidents range from credential theft and ransomware to denial-of-service and phishing campaigns, with consequences including the theft of sensitive staff and student data, disruption of teaching and research, and long-term reputational damage. The clustering of attacks around exam periods and research activities underscores the opportunistic nature of adversaries exploiting high-stakes academic timelines. Notably, recurrent ransomware incidents have caused prolonged system outages, delayed coursework, and compromised research data, demonstrating how universities' reliance on digital infrastructure makes them attractive and vulnerable targets. The figure also reveals persistent patterns credential compromises through phishing, denial-of-service disruptions, and repeated ransomware strains indicating that despite policy and awareness efforts, cyber resilience in higher education remains limited without systemic cultural and behavioral change.

Complementing this, Cheng and Wang [8] propose institution-level strategies that treat cybersecurity as a socio-technical system, recommending integrated leadership, investment in workforce competencies, and culture-building, elements often under-resourced relative to technology spend [8]. Together, this corpus converges on a central claim: HEIs are structurally exposed, and durable risk reduction depends on organizational and behavioral levers as much as on tools.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

1.2.2. From Awareness to Behaviour: Competing Explanations

The literature on human factors offers partially competing explanations for secure (and insecure) behavior. Systematic evidence indicates that the Protection Motivation Theory (PMT) dominates explanatory models in cybersecurity behavior research, with self-efficacy and response efficacy repeatedly outperforming fear appeals in predicting intentions and actions [4, 9]. Studies applying PMT in public-sector contexts (e.g., Malaysian government employees) demonstrate that responsibility and coping appraisal are significant, but their effects are contingent on organisational climate and perceived control limits that caution against purely message-based interventions [6]. In parallel, the Theory of Planned Behaviour (TPB)-based work emphasizes the role of subjective norms and perceived behavioural control; however, meta-reviews note TPB's weakness in capturing environmental constraints and habit formation, both of which are pronounced in university work routines, as shown below in Figure 1.

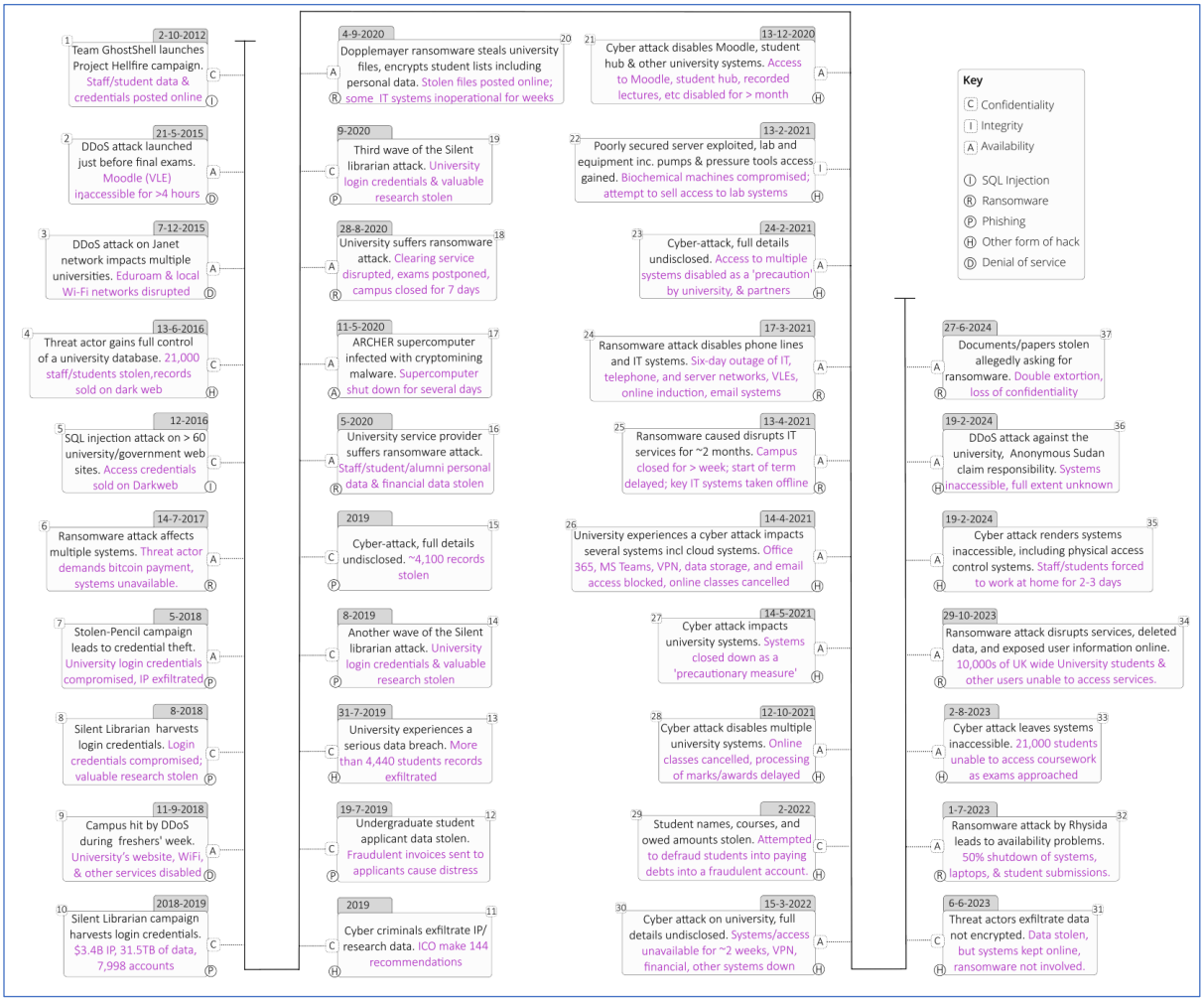

Figure 1.
History of cyberattacks in UK universities.
Source: Lallie, et al. [3].

The COM-B/Behaviour Change Wheel (BCW) perspective addresses this gap by modelling behaviour as a function of Capability, Opportunity, and Motivation, and by linking these drivers to specific intervention functions (training, enablement, environmental restructuring) and policy levers.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

Although originally developed in health contexts, its diagnostic utility has increasingly been recognised in cybersecurity pedagogy and culture programmes for HEIs [7, 10]. COM-B helps explain why employees may possess the knowledge and motivation to comply, yet fail to act securely if institutional opportunities such as usable policies, cultural reinforcement, or peer modeling are absent. This dynamic is illustrated in Figure 2, which maps partial correlations between COM-B components and specific security behaviors such as information sharing, checking recipients, encrypting files, and locking screens. The figure demonstrates that capability consistently shows strong correlations with behavior (e.g., 0.57 for locking screens), while motivation and opportunity vary in their influence across contexts (e.g., opportunity correlates more strongly with file encryption at 0.48, compared to motivation at 0.37). These findings emphasize that secure conduct in HEIs cannot be reduced to awareness alone: without structured opportunities such as supportive infrastructures, adaptive policies, and cultural reinforcement, even capable and motivated employees may default to insecure practices.

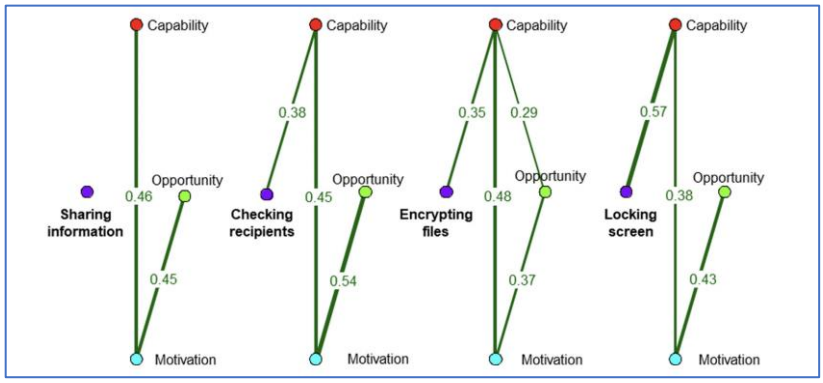

Figure 2.
Partial correlations between Capability, Opportunity, and Motivation in shaping employee data leakage prevention behaviours.
Source: van der Kleij, et al. [11].

These theoretical perspectives converge in Figure 3, adapted from Ali et al. [5], the text describes the transformation of employee behaviour from noncompliance to compliance with information security policies (ISPs). The model illustrates how organisational stressors, value conflicts, and neutralisation strategies can initially foster intentions to resist compliance. Transitioning towards compliance requires the activation of protection motivation behaviours, supported by intrinsic/extrinsic motivation, formal/informal sanctions, and critically, top management behaviours that demonstrate leadership commitment. Once this transition occurs, compliance is stabilised through social behaviours, security-aware practices, and the emergence of a good security culture, which in turn strengthens intentions to comply and leads to actual compliance with ISPs.

When viewed alongside PMT, TPB, and COM-B, the model in Figure 5 reinforces the argument that cybersecurity compliance is not reducible to cognitive risk appraisal or normative pressure alone. Rather, it emerges from a *dynamic interaction* between motivation, organisational climate, managerial influence, and cultural embedding. For HEIs, this implies that behavioural change cannot rely exclusively on awareness campaigns or rigid enforcement; it requires *multi-layered strategies* that simultaneously address psychological, organisational, and cultural drivers of behaviour.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

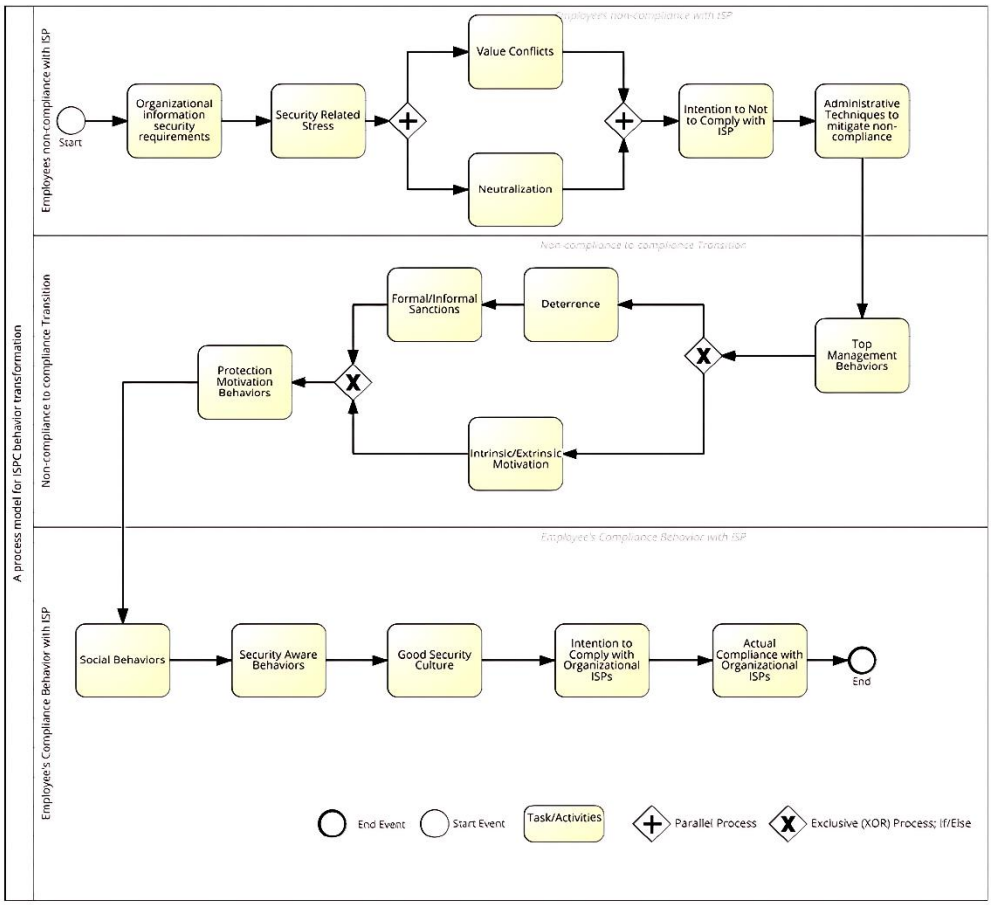

Figure 3.
Behaviour transformation from noncompliance to compliance with information security policies (ISPs).
Source: Ali, et al. [5].

1.2.3. Policy, Culture, and Maturity: Alignment Problems

Even where formal policies exist, compliance is uneven. A systematic review of information-security policy compliance (ISPC) highlights a recurrent translation problem: organizations codify rules, but employees encounter usability frictions, role ambiguity, and low procedural fit, which depress compliance and encourage workaround cultures [5]. Within academia, awareness frameworks tailored to HEIs argue for curriculum-integrated and role-specific interventions that extend beyond student cohorts to staff and faculty, the primary interpreters of policy in everyday workflows [10]. On governance, cybersecurity maturity frameworks are frequently proposed to institutionalize continuous improvement. The HCYMAF model for UK HEIs consolidates regulatory and best-practice controls into 15 categories and six maturity levels, offering a lightweight self-assessment instrument [12]. However, subsequent MDPI work and sector reviews caution that maturity scoring can drift toward checklist compliance if not linked to behavior and culture metrics; implementation studies remain less common than framework proposals, limiting evidence on real-world uplift [13]. More recent MDPI analyses propose integrated management and compliance models spanning operational, technical, human, and physical domains, explicitly attempting to remedy the fragmentation seen when policy, training, and technology progress on separate tracks [14]. The comparative message is consistent: maturity scaffolds are useful, but HEIs achieve durable gains only when policy clarity, usable controls, and culture-building reinforce one another.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

1.2.4. Attitudes in HEIs in UAE Contexts

Attitudes, risk appraisal, perceived control, and normative expectations are repeatedly identified as proximal drivers of secure practice. Sector-focused reviews and UK case syntheses report that training and communications often skew technical, while faculty and staff report deficits in practicality (e.g., policy-workflow misalignment), timeliness of IT support, and visible leadership endorsement factors that attenuate positive attitudes and create intention-behavior gaps [3, 8]. Conceptual work on HEI cybersecurity culture emphasizes sustained, audience-segmented programmes rather than one-off awareness drives, including mechanisms for feedback and co-design with academic units [7, 10]. Yet, qualitative evidence from Gulf and UAE university settings remains sparse in indexed literature; where available, studies emphasize rapid digitalization and compliance pressures but seldom focus on the lived experiences of staff who must reconcile policy with operational demands. This gap motivates the present study's qualitative focus on the attitudes of faculty and staff in UAE HEIs, using PMT, TPB, and COM-B as complementary lenses to explore how perceptions translate (or fail to translate) into everyday secure behavior.

Across MDPI and Scopus-indexed sources, three propositions emerge. First, HEI cyber risk is systemic and persistent; technology-only strategies underperform without institutional and behavioral design [1, 3, 8]. Second, among behavioural theories, PMT and TPB explain intentions, but COM-B/BCW is better suited to designing interventions that modify environments and capabilities, not just cognitions [4, 7, 9, 10]. Third, policy-culture-maturity alignment remains the binding constraint: frameworks like HCYMAF provide structure, but their impact hinges on whether policies are usable, training is contextualized for academic roles, and leadership fosters norms that make secure behavior the path of least resistance [5, 12-14]. These insights shape our study design and analysis and inform practice recommendations for UAE HEIs seeking to cultivate resilient, human-centered cybersecurity.

2. Materials and Methods

2.1. Research Design

This study adopted a qualitative research design centered on semi-structured interviews to explore faculty and staff attitudes toward cybersecurity within higher education institutions (HEIs) in the United Arab Emirates. A qualitative approach was particularly appropriate given the study's focus on uncovering underlying beliefs, experiences, and cultural contexts that are not easily reducible to quantitative measures. Semi-structured interviews were chosen as they provide both structure, ensuring alignment with the study's objectives, and flexibility, allowing participants to elaborate on issues of personal salience. This combination facilitated deeper insights into how employees interpret and enact cybersecurity policies in their institutional environments.

2.2. Participants and Sampling

Participants were purposively selected to reflect the diversity of professional roles in HEIs, including academic faculty, administrative staff, IT specialists, and senior management. This heterogeneity was critical for capturing differences in how cybersecurity policies and practices are experienced across organizational strata. A total of 20 participants took part in the interviews, representing a balanced distribution across the identified groups. Purposeful sampling also enabled the inclusion of individuals with varying years of experience, ensuring that both long-serving and relatively new employees could articulate their perspectives on evolving cybersecurity practices.

2.3. Instrumentation

The interview guide was informed by both the systematic literature review and the preliminary survey findings of the broader study, ensuring conceptual grounding and contextual relevance. The guide addressed key themes including:

- Awareness and training experiences: participants' perceptions of institutional efforts to build knowledge and competence.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

- Policy perception and applicability: the extent to which formal policies are perceived as practical and relevant.
- Daily practices and challenges: how cybersecurity behaviors were integrated, or resisted, in routine work.
- Institutional culture and peer influence: the role of collective norms and informal practices in shaping behavior.
- Technological and infrastructural support: perceptions of system readiness and IT responsiveness.
- Feedback mechanisms: opportunities for staff to contribute to policy refinement and awareness initiatives.

Crucially, the structure of the interview guide was directly aligned with the aim of the study, to understand how attitudes shape secure and insecure cybersecurity practices in HEIs, and the corresponding research questions. For example, questions on training and awareness explored how institutional interventions influenced employee attitudes, thereby addressing the research aim of linking policy communication to behavioural outcomes. Similarly, items on daily practices, cultural dynamics, and peer influence were designed to probe the psychological and social dimensions of cybersecurity behaviour, consistent with the theoretical framing of Protection Motivation Theory (PMT), the Theory of Planned Behaviour (TPB), and the COM-B model. The guide ensured coherence between data collection and the broader analytical objectives of the study.

To enhance *validity*, the interview guide was reviewed by two experts in cybersecurity and educational research, who provided feedback on the clarity, comprehensiveness, and relevance of the questions. A pilot with two participants was then conducted, allowing refinement of question wording and sequencing to ensure accessibility and reduce ambiguity. *Reliability* was strengthened through consistent use of the same core guide across all interviews, while the semi-structured format permitted follow-up probes without compromising comparability. Furthermore, reflexive documentation and intercoder checks during analysis ensured that the data derived from the guide were interpreted systematically and with minimal researcher bias.

2.4. Data Collection

Interviews were conducted online, allowing participation from across institutions while maintaining consistency in delivery. Each session lasted between 45 and 60 minutes, providing sufficient scope for participants to articulate their views without imposing an excessive burden. The virtual format also enabled a diverse sample to be included despite geographical and scheduling constraints.

Audio-recorded interviews were transcribed verbatim and subsequently anonymized to ensure confidentiality. Transcripts were reviewed iteratively to check for accuracy and completeness. While minor disfluencies were retained to preserve meaning, irrelevant fillers were removed to support clarity during analysis. Each transcript was assigned a unique identifier, allowing for systematic coding and analysis without compromising participant anonymity.

2.5. Data Analysis

Thematic analysis was conducted following Braun and Clarke's six-phase framework, which provides both methodological rigour and interpretive flexibility. Initial coding was conducted inductively to capture emergent patterns, while subsequent stages involved refining themes in light of both the coded extracts and the broader dataset. Three overarching thematic clusters were identified: (1) institutional communication and training, (2) policy-practice misalignments, and (3) cultural and peer influences on behaviour. Within each cluster, subthemes highlighted more nuanced dynamics, such as the perceived irrelevance of generic training modules or the role of informal peer norms in reinforcing or undermining policy compliance.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

To ensure analytical robustness, coding decisions were periodically cross-checked with an independent researcher, and reflexive notes were maintained to track how researcher assumptions might shape interpretation. Data sufficiency was assessed through *saturation*, with no substantively new themes emerging after the final interviews.

3. Results

The analysis of the semi-structured interviews revealed three interrelated themes: (1) Institutional Communication and Training, (2) Policy–Practice Misalignment, and (3) Cultural and Peer Influences on Behaviour. These themes reflect how employee attitudes toward cybersecurity are shaped not merely by individual awareness but by the institutional environment in which policies, practices, and norms are embedded. Table 1 summarises the themes, codes, and illustrative meanings. Table 1 reveals a self-reinforcing loop: superficial training (Theme 1) fails to build confidence, making rigid processes (Theme 2) feel costlier and less negotiable; those frictions then feed a culture of circumvention (Theme 3), which in turn lowers expectations for meaningful training and usable policy. At the same time, the table also signals practical points of intervention: role-specific reinforcement and follow-up (Theme 1), risk-tiered flexibilities and faster approvals (Theme 2), and leadership modelling with real feedback loops (Theme 3). In short, the table does more than catalogue codes; it maps the micro-to-macro dynamics through which attitudes crystallise into (in)secure practice.

Table 1.
Summary of Themes and Codes Derived from Semi-Structured Interviews.

Theme	Codes	Illustrative Meaning
1. Institutional Communication and Training	- "Generic awareness sessions" - "Tick-box training" - "No follow-up after training" - "Too technical or too simplistic" - "Cybersecurity mentioned only after incidents."	Training initiatives were perceived as symbolic rather than substantive, failing to connect with daily professional realities. The absence of reinforcement mechanisms and routine communication undermined coping appraisal, leaving employees skeptical of their ability to enact secure behaviors.
2. Policy–Practice Misalignment and the Paradox of Control	- "Policies slow us down" - "Use of personal/unauthorised devices" - "No flexibility in adopting new tools" - "Lengthy IT approval processes" - "Rejecting obstructive policies, not security itself"	Policies were described as rigid and poorly adapted to academic workflows, fostering practical non-compliance. Employees acknowledged the importance of cybersecurity but rejected institutional mechanisms that obstructed productivity and innovation, undermining perceived behavioral control.
3. Cultural and Peer Influences on Behaviour	- "Cybersecurity is the IT department's problem." - "Peers ignore rules without consequences" - "Leadership modelling improves compliance" - "No feedback channels for staff input" - "Culture of circumvention normalised"	Cybersecurity attitudes were strongly shaped by peer norms and cultural framing. In weak cultural environments, employees normalized non-compliance when rules were routinely bypassed without consequence. Conversely, leadership modeling and participatory governance fostered shared responsibility and strengthened security culture.

3.1. Institutional Communication and Training

A strong consensus among participants was that cybersecurity training in higher education institutions (HEIs) was symbolic rather than substantive. Many described training sessions as generic, superficial, and disconnected from their work realities.

> *"After the session, there is no follow-up. Nobody checks if you really applied what you learned." (Participant 02)*

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

"We receive occasional training, but it feels more like ticking a box than actually preparing us for real risks." (Participant 07)

"The material is too technical at times, and at other times overly simplistic. It doesn't connect with what we actually face in our day-to-day work." (Participant 14)

This finding aligns with Khader et al. [7], who argue that awareness frameworks in academia remain largely ineffective because they fail to contextualise cybersecurity in the lived experience of staff and faculty. The absence of differentiation between professional roles undermines engagement: academic staff often see policies as irrelevant to teaching and research, while administrative staff perceive training as overly technical. Cheng and Wang [8] similarly emphasize the importance of tailoring cybersecurity interventions to the user's professional environment to avoid disengagement.

Several participants highlighted that training was treated as a one-off exercise, with no reinforcement mechanisms:

"It's like a one-time lecture. By the time the next session comes around, you've already forgotten half of it." (Participant 15)

This finding resonates with research by Sommestad and Karlzén [15] and Adams and Makramalla [9], who show that interactive, continuous, and gamified training strategies produce more sustainable behavioural change compared to episodic, lecture-based formats. From a PMT perspective, training in these HEIs fails to build coping appraisal, particularly self-efficacy and response efficacy, meaning that employees remain unconvinced that they can effectively prevent or mitigate threats.

The interviews also indicated a lack of institutional signaling: cybersecurity is not positioned as an organizational priority. As one participant noted:

"We hear about cybersecurity only when something bad happens. It's not part of the regular conversation." (Participant 04)

This absence of consistent communication undermines institutional credibility. Literature on higher education cybersecurity emphasizes that communication strategies must reinforce collective responsibility and maintain visibility across the organization [12, 14]. Without this, employees perceive cybersecurity as peripheral, and their attitudes reflect skepticism rather than commitment.

3.2. Policy-Practice Misalignment

Another central theme was the disconnect between cybersecurity policies and academic practice. Participants repeatedly described policies as rigid, slow to adapt, and poorly aligned with pedagogical and administrative workflows.

"The policies look good on paper, but in practice they slow us down. Sometimes we ignore them just to get the job done." (Participant 03)

"Sometimes we use our own devices because the approved ones are outdated or restricted. It's easier to take the risk than wait weeks for IT approval." (Participant 05)

"There is no room for flexibility. If I want to use a new tool for teaching, the approval process is so long that I just end up bypassing it." (Participant 11)

This echoes the conclusions of Uchendu et al. [12], who demonstrate that HEIs remain vulnerable not because of absent policies but because those policies are detached from operational realities. Similarly, Ali et al. [5] and Yazdanmehr et al. [10] describe this phenomenon as "practical non-compliance": employees do not reject security in principle but actively bypass rules when they conflict with productivity.

The interviews also revealed frustration with bureaucratic approval processes that hindered innovation in teaching and research. One faculty member explained:

"I wanted to use a cloud-based platform for a collaborative project, but it took months to get clearance. By the time we got approval, the project had already moved on." (Participant 13)

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

Such findings illustrate the challenge of balancing security with academic freedom, a tension unique to universities. From a TPB perspective, these institutional constraints reduce perceived behavioral control, leading to attitudinal disengagement and behavioral non-compliance [13].

This theme also underscores a paradox: employees acknowledge the importance of cybersecurity but view current mechanisms as obstructive rather than enabling. As one participant observed:

"I don't reject security, but I reject policies that make my work impossible. Security should support us, not block us." (Participant 10)

This reflects Ulven and Wangen [1] and Parsons et al. [14], argument that universities require contextualized, adaptive policies that integrate with the specific workflows of faculty, staff, and students. Without this, formal compliance frameworks risk undermining trust and reinforcing a culture of circumvention.

3.3. Cultural and Peer Influences on Behaviour

The third theme highlights the role of organizational culture and peer norms in shaping cybersecurity attitudes and practices. Many participants described a culture where cybersecurity was seen as the exclusive responsibility of the IT department.

"Cybersecurity isn't part of the culture here. It feels like something external that we comply with only when necessary." (Participant 18)

"People see others ignoring rules and facing no consequences. That sends the message that compliance is optional." (Participant 12)

This aligns with Alsharida et al. [16], who argue that weak cybersecurity culture is among the most critical vulnerabilities in HEIs. When employees perceive cybersecurity as an external imposition, compliance becomes superficial and situational. van Steen et al. [17] similarly show that peer influence often outweighs formal policy, with norms of non-compliance spreading quickly in environments where sanctions are absent.

Notably, some participants emphasised the positive role of leadership and peer modelling:

"When my department head takes security seriously, we all pay more attention. Leadership attitude makes a big difference." (Participant 06)

This demonstrates that while culture can undermine security, it can also act as a powerful enabler when norms are modeled from the top down. In line with the COM-B framework, this reflects the opportunity dimension: cultural reinforcement creates or constrains the conditions for secure behaviors.

A recurring issue was the absence of feedback channels, which reinforced disengagement:

"We are never asked what works or doesn't work. Policies just arrive, and we have to adapt, even if they don't fit." (Participant 01)

This finding supports van Steen [18], who demonstrates that participatory governance in cybersecurity policy-making increases ownership and compliance. Without such mechanisms, employees in UAE HEIs feel excluded from decision-making, reinforcing the perception that cybersecurity is a top-down mandate rather than a shared responsibility.

Overall**,** the results demonstrate that cybersecurity attitudes in UAE HEIs are shaped not by ignorance but by institutional shortcomings in communication, policy design, and cultural embedding. Employees value security in principle but disengage when practices are perceived as irrelevant, obstructive, or externally imposed. In line with prior research, Khader et al. [7], Uchendu et al. [12], and Parsons et al. [14], these findings suggest that effective cybersecurity in HEIs requires human-centered, context-sensitive, and participatory approaches, integrating communication, policy flexibility, and cultural reinforcement.

4. Discussion

This study examined cybersecurity attitudes among faculty and staff in UAE higher education institutions (HEIs), revealing how institutional communication, policy design, and cultural dynamics

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

shape secure and insecure practices. The findings demonstrate that employees generally recognize the importance of cybersecurity but disengage when interventions are perceived as irrelevant, obstructive, or externally imposed. The following discussion situates these themes within behavioral theory and existing literature, highlighting theoretical contributions and practical implications.

4.1. Communication, Training, and the Limits of Awareness

The results indicate that training programmes are perceived as generic, symbolic, and disconnected from practice, echoing prior work that highlights the limited effectiveness of awareness campaigns in academia when not contextually grounded [7, 8]. In PMT terms, such training fails to activate coping appraisal; employees question whether they possess the capability and the efficacious responses to act securely, even if threat appraisal is present. Consistent with this, sustained, interactive, and context-relevant approaches (e.g., scenario-based, role-tailored, or gamified formats) show more durable effects than one-off lectures [9], and meta-level syntheses suggest that training must be embedded in a continuous learning cadence to maintain behavior change [11, 19].

The interviews also revealed weak institutional signaling; cybersecurity is discussed predominantly post-incident, which dampens motivation. This aligns with evidence that proactive, routine communication strengthens the salience of cybersecurity as part of one's professional role rather than an administrative add-on [13]. Beyond messaging cadence, measurement matters: security culture instruments such as HAIS-Q demonstrate that tailored interventions can target low-scoring dimensions (e.g., email handling, password behaviors, incident reporting) and track change over time [19-21]. In HEIs, where roles are heterogeneous, role-sensitive design faculty, administrative, and IT appears critical to convert awareness into enacted practice [7, 12, 14].

Implication: HEIs should pivot from compliance-oriented awareness to programmatic behaviour change: (i) role-specific content, (ii) periodic boosters tied to threat landscape and academic calendars, (iii) interactive drills or simulations, and (iv) instrumentation (e.g., HAIS-Q) to monitor attitude/behaviour shifts.

4.2. Policy-Practice Misalignment and the Paradox of Control

A central paradox is that employees endorse cybersecurity in principle yet resist inflexible processes. Interviews described slow approvals for new tools, usability frictions, and blanket restrictions that impede teaching/research. This maps to TPB's perceived behavioral control: even with favorable attitudes and norms, restrictive mechanisms depress intentions to comply. The literature calls this "practical non-compliance," workarounds adopted to preserve productivity when policy usability is low [10]. University-sector evidence similarly shows that attacks and vulnerabilities persist not for lack of policy, but because policies are detached from operational realities (e.g., identity management, bring-your-own-device, research collaboration tooling) [12, 14].

Recent work stresses adaptive policy architectures, principle-based baselines with risk-assessed exceptions, pilotable micro-policies, and short review cycles to better fit HEI workflows [8, 12]. Reviews that compare policy maturity with lived practice caution against checklist compliance; maturity needs links to behavioral and culture metrics to avoid paper security [12]. Emerging behavioral strategy research further advocates five-step approaches that start with behavior diagnosis, co-design interventions, and iterate with evidence [22].

Implication: For UAE HEIs, participatory co-design, "safe-to-try" sandboxes, and explicit exception pathways can preserve academic agility while maintaining institutional resilience. Policies should be usable by design, minimising friction where risk is low, concentrating controls where risk is material.

4.3. Culture, Peer Influence, and the Social Dynamics of Compliance

Participants frequently framed cybersecurity as "the IT department's problem," indicating weak shared ownership and powerful peer modeling effects. Where colleagues circumvent controls without consequence, non-compliance becomes normalized, an observation echoed in field studies showing social

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

influence as a stronger predictor of policy adherence than awareness alone [17]. Sector analyses likewise argue that weak cyber culture amplifies institutional exposure because informal norms override formal structures [16].

The COM-B lens clarifies why knowledge (capability) and positive attitudes (motivation) may still fail to translate into behaviour when opportunity, the social and environmental affordances, is misaligned. Leadership modelling and participatory governance (e.g., involving staff in policy shaping, visible recognition of secure behaviours, transparent incident learning) can reconstitute the opportunity structure and shift norms [18]. Reviews across human-factor cybersecurity converge on the same point: culture is the multiplier that makes technical and policy controls effective [17, 23-25].

Implication: Cultural embedding requires (i) visible leadership exemplars, (ii) peer reinforcement (e.g., champions within departments), (iii) feedback channels with actioning of inputs, and (iv) consistent consequence management that is educative rather than punitive.

4.4. Theoretical Contributions

The findings demonstrate how PMT, TPB, and COM-B jointly explain the attitude–behaviour gap in HEIs. PMT highlights the coping shortfall in generic training (self-efficacy, response efficacy). TPB clarifies how perceived control is undermined by rigid processes. COM-B explains how opportunity (culture/peer norms) governs enactment even when capability and motivation are present. Recent empirical work reinforces these linkages, e.g., PMT's strong predictive power across device contexts [26] and meta-reviews that integrate multiple human-factor theories to build multi-layered interventions [23-25]. The resulting model (Figure 1) therefore reframes HEI cybersecurity as a behavioral system: interventions must be coherent across capability, control, and opportunity to shift attitudes into sustained secure practice.

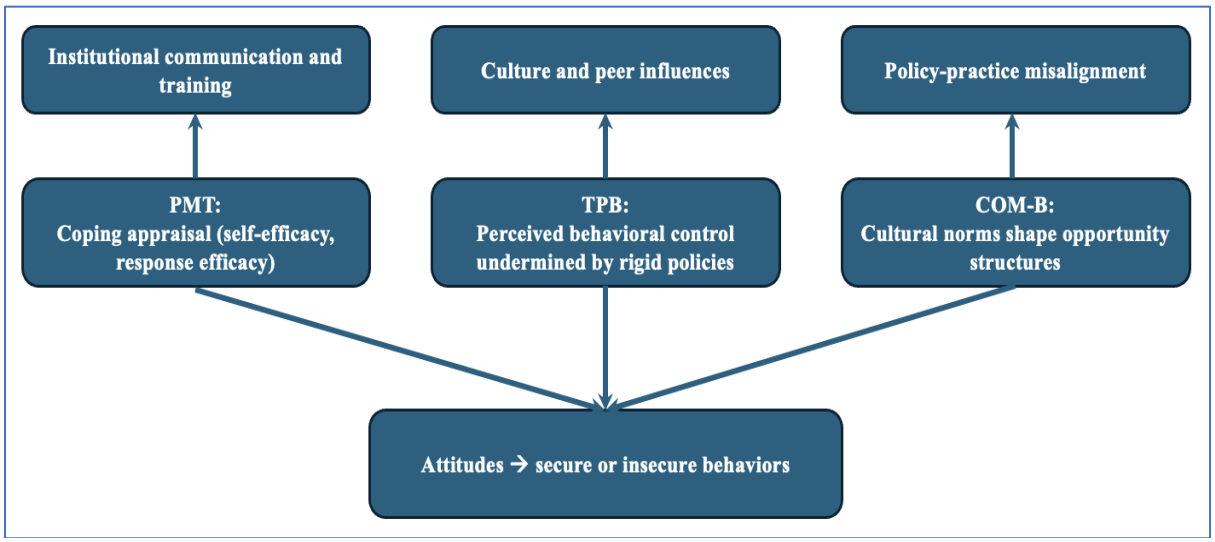

Figure 4.
Conceptual Model: Cybersecurity Attitudes of HEI in the UAE.

4.5. Practical Implications for UAE HEIs

For institutional leaders and policymakers, several actionable implications arise:

1. Role-Specific Training: Replace generic awareness with tailored modules for faculty, administrators, IT staff, and management, with interactive drills and periodic refreshers [7, 9, 19, 20].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

2. Adaptive Policy Design: introduce co-design and feedback loops; employ risk-tiered controls, rapid exception handling, and pilotable changes to minimize friction while maintaining assurance [8, 10, 12, 14, 22].
3. Cultural embedding: position cybersecurity as a shared institutional value through leadership modeling, peer champions, recognition of good practice, and learning-oriented incident reviews [16-18, 23, 27].
4. Participatory Governance: Establish staff forums and feedback channels; communicate actions taken on feedback to build psychological ownership and trust [18].
5. Measurement & Iteration: Use validated instruments (e.g., HAIS-Q) and maturity frameworks (e.g., HCYMAF) to baseline culture/behavior, then iterate interventions based on data [12, 19-21, 25, 27].

Such measures would not only improve compliance but also cultivate a culture where cybersecurity is an integral part of the academic mission rather than an external constraint.

5. Conclusion

This study examined cybersecurity attitudes among faculty and staff in higher education institutions in the United Arab Emirates, with a focus on how institutional practices, policy frameworks, and cultural dynamics shape secure and insecure behaviors. Through qualitative interviews, three interrelated themes emerged: the inadequacy of communication and training, the misalignment between policy and practice, and the decisive role of cultural and peer influences.

The findings highlight that disengagement from cybersecurity in HEIs does not stem from ignorance but from systemic shortcomings. Training programmes are often symbolic, providing awareness without enhancing coping appraisal. Policies, though well intentioned, are frequently rigid and obstructive, diminishing employees' perceived behavioural control. Organisational culture too often relegates cybersecurity to the IT department, reinforcing norms of non-compliance when peers circumvent rules without consequence. Together, these dynamics illustrate how institutional structures and cultural contexts mediate the translation of attitudes into behaviours.

By mapping the results onto Protection Motivation Theory (PMT), the Theory of Planned Behaviour (TPB), and the COM-B framework, the study advances the theoretical understanding of cybersecurity as a behavioral phenomenon rather than a purely technical challenge. The conceptual model developed here demonstrates how employee attitudes are shaped through interconnected pathways of communication, policy, and culture, converging to influence either secure or insecure practices.

For UAE HEIs, the practical implications are clear. Institutions should move beyond one-size-fits-all awareness campaigns, implementing role-specific, continuous training that links directly to professional realities. Policies must be adaptive and developed through participatory processes that balance compliance with flexibility, thereby increasing ownership and reducing circumvention. Finally, cultivating a strong cybersecurity culture requires visible leadership modeling, peer reinforcement, and mechanisms that embed cybersecurity as a shared institutional responsibility.

Future research should extend this analysis by exploring cross-cultural comparisons between HEIs in different regions and integrating longitudinal data to examine how attitudes and behaviors evolve over time. Such work would further clarify the dynamic interplay between institutional structures, employee attitudes, and behavioral outcomes.

In sum, the study provides empirical evidence that cybersecurity in HEIs is as much a matter of behavioral and cultural design as it is of technical policy. Addressing the attitudinal drivers of secure and insecure practices is essential if universities in the UAE, and globally, are to build resilience in an increasingly complex threat landscape.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

References

[1] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, p. 39, 2021. https://doi.org/10.3390/fi13020039

[2] National Cyber Security Centre (NCSC), "Cyber security for higher education institutions," 2022. https://www.ncsc.gov.uk/section/education-skills/cyber-security-heis-feis

[3] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, "Analysing cyber attacks and cyber security vulnerabilities in the university sector," *Computers*, vol. 14, no. 2, p. 49, 2025. https://doi.org/10.3390/computers14020049

[4] A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories," *Applied Sciences*, vol. 13, no. 9, p. 5700, 2023. https://doi.org/10.3390/app13095700

[5] R. F. Ali, P. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance," *Applied Sciences*, vol. 11, no. 8, p. 3383, 2021. https://doi.org/10.3390/app11083383

[6] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks," *Information*, vol. 13, no. 9, p. 413, 2022. https://doi.org/10.3390/info13090413

[7] M. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," *Information*, vol. 12, no. 10, p. 417, 2021. https://doi.org/10.3390/info12100417

[8] E. C. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, p. 192, 2022. https://doi.org/10.3390/info13040192

[9] M. Adams and M. Makramalla, "Cybersecurity skills training: An attacker-centric gamified approach," *Technology Innovation Management Review*, vol. 5, no. 1, pp. 5–14, 2015.

[10] A. Yazdanmehr, J. Wang, and Z. Yang, "Peers matter: The moderating role of social influence on information security policy compliance," *Information Systems Journal*, vol. 30, no. 5, pp. 791-844, 2020. https://doi.org/10.1111/isj.12271

[11] R. van der Kleij, K. Schraagen, and L. Taal, "An application and empirical test of the COM-B model to data-leakage prevention behaviours," *Computers & Security*, vol. 97, p. 101935, 2020.

[12] B. Uchendu, J. R. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," *Computers & Security*, vol. 109, p. 102387, 2021. https://doi.org/10.1016/j.cose.2021.102387

[13] K. L. Gwebu, J. Wang, and M. Y. Hu, "Information security policy noncompliance: An integrative social influence model," *Information Systems Journal*, vol. 30, no. 2, pp. 220-269, 2020. https://doi.org/10.1111/isj.12257

[14] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Computers & Security*, vol. 66, pp. 40-51, 2017. https://doi.org/10.1016/j.cose.2017.01.004

[15] T. Sommestad and H. Karlzén, "Employees' knowledge and training in information security: Effects on security behavior," *Computers & Security*, vol. 39, pp. 60–70, 2013.

[16] A. R. Alsharida, A. Hammouri, and H. Alzoubi, "A systematic review of multi-perspectives on human cybersecurity behaviour," *Evaluation and Program Planning*, vol. 99, p. 102322, 2023.

[17] T. van Steen, B. van den Berg, and J. Prümmer, "Assessing the effect of cybersecurity training on end-users: A meta-analysis," *Computers & Security*, vol. 150, p. 104206, 2024.

[18] T. van Steen, "Developing a behavioural cybersecurity strategy: A five-step approach for organisations," *Computer Standards & Interfaces*, vol. 92, p. 103939, 2025. https://doi.org/10.1016/j.csi.2024.103939

[19] U. Kiran, N. F. Khan, H. Murtaza, A. Farooq, and H. Pirkkalainen, "Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory," *Computers & Security*, vol. 149, p. 104204, 2025. https://dl.acm.org/doi/10.1016/j.cose.2024.104204

[20] K.-M. Kuo, C. Talley, and C.-M. Lai, "A meta-analysis of the deterrence theory in security compliance," *Computers & Security*, vol. 96, p. 101837, 2020.

[21] R. Armas and H. Taherdoost, "Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm," *Information*, vol. 16, no. 5, p. 336, 2025. https://doi.org/10.3390/info16050336

[22] M. Antunes, C. Silva, and F. Marques, "An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context," *Applied Sciences*, vol. 11, no. 23, p. 11269, 2021. https://doi.org/10.3390/app112311269

[23] M. A. Alqahtani, "Factors affecting cybersecurity awareness among university students," *Applied Sciences*, vol. 12, no. 5, p. 2589, 2022. https://doi.org/10.3390/app12052589

[24] S. Mahmood, M. Chadhar, and S. Firmin, "Addressing cybersecurity challenges in times of crisis: Extending the sociotechnical systems perspective," *Applied Sciences*, vol. 14, no. 24, p. 11610, 2024. https://doi.org/10.3390/app142411610

[25] S. Badreddine, A. Alazzam, A. Omari, H. Alammari, and G. Khalifa, "The use of artificial intelligence in cyber security," in *Proceedings of the International Conference on Computing and Information Technology (ICCIT - 25). Casablanca, Morocco*, 2025.

[26] A. Aliyu *et al.*, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Applied Sciences*, vol. 10, no. 10, p. 3660, 2020. https://doi.org/10.3390/app10103660

[27] S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Computers & Security*, vol. 31, no. 8, pp. 983-988, 2012. https://doi.org/10.1016/j.cose.2012.08.004

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10: 439-453, 2025
DOI: 10.55214/2576-8484.v9i10.10445