Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Cybersecurity Awareness for AI-Enabled Learning Environments: Evidence from Higher Education Institutions in Kuwait

Abdullah F Alenezi

af.alenezi@paaet.edu.kw

Public Authority for Applied Education and Training

Research Article

Keywords: Cybersecurity awareness, AI-enabled learning, Learning analytics, Cyber threat knowledge, Cybersecurity practices, Digital learning resilience, Higher education, Kuwait

Posted Date: August 25th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10296063/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Artificial intelligence (AI), learning analytics, and digital learning platforms are transforming higher education by enabling personalised learning, automated assessment, and data-informed decision-making. These developments rely on secure and trustworthy digital environments, yet empirical evidence on the human dimensions of cybersecurity within Gulf Cooperation Council (GCC) higher education institutions remains limited. This study investigated the relationships between cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices among staff and students in Kuwaiti higher education institutions, while considering their implications for AI-enabled learning.

A cross-sectional survey was conducted with 270 participants from seven higher education institutions in Kuwait. Data were analysed using descriptive statistics, Spearman's rank correlation, and ordinal logistic regression. The measurement instrument demonstrated satisfactory reliability (Cronbach's α = .870). Cybersecurity knowledge and cyber threat knowledge were both positively associated with cybersecurity practices (ρ = .422 and ρ = .420, respectively; $p < .001$), while also showing a moderate positive association with each other (ρ = .543, $p < .001$). Ordinal logistic regression confirmed that both constructs independently predicted cybersecurity practices (Cybersecurity Knowledge: $B = .943$, $p < .001$; Cyber Threat Knowledge: $B = .520$, $p < .001$), supporting the study's central hypothesis.

The findings demonstrate that cybersecurity knowledge and threat awareness are significant predictors of secure digital behaviour, while highlighting gaps in formal cybersecurity training and the translation of knowledge into practice. The study contributes empirical evidence from an underrepresented regional context and proposes a conceptual framework positioning cybersecurity awareness as a foundation for trustworthy AI-enabled learning, digital learning resilience, and educational quality. The findings provide practical recommendations for higher education institutions and inform policy development supporting Kuwait Vision 2035 and the National Cybersecurity Strategy.

1. Introduction

1.1 AI-Enabled Teaching and Learning

Higher education institutions worldwide are undergoing a period of rapid digital transformation, accelerated by the widespread adoption of cloud-based learning management systems, online assessment platforms, and — increasingly — artificial intelligence (AI). Generative AI applications such as ChatGPT, Microsoft Copilot, and Google Gemini, alongside AI-enhanced learning management systems and intelligent tutoring tools, are being adopted by students and academic staff for tasks ranging from academic writing support and programming assistance to lesson preparation and personalised feedback (UNESCO, 2023; Crompton & Burke, 2024). Luckin et al. (2016) describe this potential as the promise of intelligent tutoring, adaptive group formation, and timely feedback delivered at a scale no individual teacher can match, while Zawacki-Richter et al. (2024) note that AI is increasingly used across the full span of the student lifecycle, from admissions and advising to assessment and

student support. Selwyn (2019) cautions, however, that these technologies also raise unresolved questions about the social, emotional, and pedagogical roles that should remain with human teachers rather than being delegated to automated systems.

These educational benefits — adaptive learning, automated feedback, and improved institutional decision-making — depend on the continuous collection and processing of large volumes of educational data. As universities become more data-intensive teaching organisations, the trustworthiness of the digital environment in which learning takes place becomes an educational concern as much as a technical one: students and staff cannot benefit from AI-enabled learning tools they do not trust, or that expose their academic and personal data to misuse. Interconnected digital platforms, cloud infrastructure, and — where adopted — AI systems widen the attack surface available to malicious actors, making cybersecurity an enabler, or a barrier, of educational innovation rather than a purely technical back-office concern.

1.2 Learning Analytics, Educational Data, and Trust in Learning

Learning analytics refers to the measurement, collection, analysis, and reporting of data about learners and their contexts, for the purpose of understanding and optimising learning and the environments in which it occurs (Siemens & Baker, 2012). Modern learning management systems such as Blackboard, Canvas, and Moodle routinely capture login frequency, attendance, assessment submissions, discussion participation, and navigation behaviour, and institutions increasingly use these data to identify students at risk of underperformance and to inform academic support (Ifenthaler & Schumacher, 2023). Williamson (2017) argues that this growth in educational data mining has outpaced the development of the ethical and governance frameworks needed to use it responsibly, while Ifenthaler and Schumacher (2023) highlight that student trust in learning analytics is itself contingent on perceived data security and transparency.

This growth in the volume and granularity of educational data held by universities increases the value of institutional systems as targets for cybercriminals, and it raises the stakes of any cybersecurity failure for teaching and learning specifically: a breach that exposes assessment records, disability disclosures, or behavioural data does more than create legal liability — it can undermine student engagement, discourage help-seeking, and erode the trust on which personalised, data-informed teaching depends. Protecting these data is therefore a strategic priority for digitally transforming universities generally, and is likely to become more, not less, important as AI-enabled analytics become more common in the classroom.

1.3 Secure Learning Environments and the AI-Enabled Threat Landscape

The cybersecurity threat landscape facing universities is evolving alongside the educational technologies they adopt. Beyond conventional threats such as phishing, malware, ransomware, and

password compromise, the security literature increasingly describes AI-specific risks: AI-generated phishing and social engineering messages that are harder to distinguish from legitimate communication, deepfake audio and video used for impersonation and fraud, and technical attacks against AI systems themselves such as prompt injection, data poisoning, model inversion, and adversarial manipulation (World Economic Forum, 2025; NIST, 2024; ENISA, 2024). Universities that adopt learning analytics platforms and generative AI tools inherit these risks in addition to the threats their information systems have always faced, and these risks translate directly into classroom concerns: compromised student accounts undermine academic integrity in AI-assisted assessment, and insecure AI tools can leak the coursework, feedback, or personal data students share with them.

It is important to be precise about what this means for the present study: these AI-specific threats describe the wider educational landscape within which cybersecurity awareness now operates, and they motivate why the topic matters for AI-enabled institutions and the staff and students who teach and learn within them. They are not constructs that this study's survey instrument measured, and the empirical findings reported below should not be read as evidence about AI-specific threat recognition. That distinction is maintained explicitly throughout the paper.

1.4 AI-Enabled Higher Education in Kuwait

Kuwait has positioned digital transformation, including AI adoption, at the centre of its national development agenda through Kuwait Vision 2035, which seeks to diversify the economy and modernise public services — including education — through digital innovation. Following the COVID-19 pandemic, higher education institutions in Kuwait accelerated their adoption of online and hybrid learning, digital assessment, and — more recently — generative AI tools used informally by students and staff in coursework, revision, and academic writing. Kuwait's National Cybersecurity Strategy recognises human capability development as essential to protecting national digital infrastructure, but existing cybersecurity initiatives have concentrated primarily on technical controls and general awareness programmes, with comparatively little empirical attention paid to cybersecurity awareness specifically within the higher education sector, or to what it means for the safe adoption of AI-enabled teaching and learning.

1.5 Research Gap, Objectives, and Contributions

Research on AI in education, learning analytics, and cybersecurity awareness has developed largely along separate tracks: AI-in-education research emphasises pedagogy, personalisation, and technology acceptance (Holmes et al., 2022; Zawacki-Richter et al., 2024); learning analytics research emphasises predictive modelling, student retention, and — increasingly — governance and ethics (Ifenthaler & Schumacher, 2023; Williamson, 2017); and cybersecurity research emphasises awareness, policy compliance, and security behaviour. Comparatively few studies examine the human dimensions of cybersecurity within Gulf higher education institutions specifically, and fewer still discuss these dimensions as a condition for safe, trustworthy AI-enabled learning.

This study addresses that gap by providing empirical evidence on cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices among staff and students in Kuwaiti HEIs, and by discussing what these findings imply — conceptually and pedagogically — for institutions navigating AI adoption. The study pursues three objectives:

- To evaluate levels of cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices among students and staff across higher education institutions in Kuwait.
- To examine the statistical relationships between cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices, testing whether the first two predict the third.
- To discuss the implications of these findings for cybersecurity awareness programmes, responsible AI use in teaching and learning, and digital learning resilience in higher education, and to propose an educational conceptual agenda for future research that would test AI-specific constructs directly.

The study contributes empirical evidence from an underrepresented regional context, a rigorously tested statistical model of the relationships among core cybersecurity constructs, and a clearly delineated conceptual discussion connecting these findings to the broader — but not yet empirically tested — questions raised by AI-enabled teaching and learning.

2. Literature Review

2.1 AI-Supported Learning

Artificial intelligence has moved from a specialist research field into a mainstream educational technology supporting teaching, learning, research, and institutional administration (Holmes et al., 2022; Zawacki-Richter et al., 2024). Luckin et al. (2016) describe intelligent tutoring systems, adaptive group formation, and AI-supported feedback as central applications through which AIEd (AI in education) aims to personalise learning at scale. The public availability of generative AI tools since 2022 has accelerated adoption by students, who use these tools for brainstorming, explanation, writing support, and code generation, and by staff, who use them for materials development, assessment design, and feedback (Kasneci et al., 2023). Selwyn (2019) argues that the more urgent question is not whether AI can replicate teaching, but which parts of the educational relationship should remain distinctly human, and how institutions should govern the parts that are delegated to machines. AI adoption also raises concerns about academic integrity, algorithmic bias, and data privacy, and requires institutions to develop AI literacy — the capacity to use AI tools critically, understand their limitations, and evaluate their outputs — alongside conventional digital literacy (UNESCO, 2023).

Much of this literature focuses on pedagogical effectiveness and technology acceptance, with comparatively limited attention paid to how AI adoption changes institutional cybersecurity requirements, or to what secure digital behaviour students and staff need in order to use AI-supported learning tools safely — a gap this study seeks to address at the level of discussion, if not direct measurement.

2.2 Learning Analytics Ethics and Data-Driven Decision-Making

Learning analytics has become central to student success initiatives, enabling institutions to identify disengaged learners and provide targeted support (Siemens & Baker, 2012; Ifenthaler & Schumacher, 2023). AI has expanded these capabilities from descriptive to predictive and, in some institutions, prescriptive analytics. Williamson (2017) situates this expansion within a broader critique of data-driven education, arguing that the same infrastructures that enable personalised support also enable forms of surveillance and algorithmic governance that are rarely made visible to the students and staff whose data are collected. The same data that make learning analytics valuable — detailed behavioural, academic, and engagement profiles — also make it a high-value target for cybercriminals, and several scholars have argued that educational data warrant governance comparable to that applied in healthcare and finance. As with AI adoption generally, the learning analytics literature has given considerably more attention to predictive validity and educational effectiveness than to cybersecurity implications, even as ethical use of learning analytics is increasingly recognised as inseparable from secure handling of the underlying data.

2.3 Digital Resilience in AI-Enabled Learning Environments

The education sector is consistently identified as one of the most frequently targeted industries globally, owing to the combination of valuable personal and institutional data with relatively open network environments that support collaboration and academic freedom (ENISA, 2024; IBM Security, 2024). As discussed in Section 1.3, generative AI has introduced new categories of risk — more convincing phishing and social engineering, deepfake-enabled fraud, and attacks targeting AI systems directly (prompt injection, data poisoning, model inversion, adversarial manipulation). Universities that adopt cloud-hosted AI platforms and third-party learning analytics services also inherit supply-chain and cross-border data-transfer risks associated with those vendors, with direct consequences for the continuity of teaching, assessment, and student support if systems are disrupted.

Early cybersecurity awareness research defined the construct primarily as users' knowledge of threats and their adoption of safe practices such as strong passwords and phishing recognition (Kruger & Kearney, 2006; Ifinedo, 2012). More recent work situates cybersecurity awareness within the broader concept of digital resilience — an organisation's capacity to anticipate, withstand, respond to, and recover from digital disruption, rather than simply preventing incidents. For a university, digital resilience is inseparable from educational continuity: the ability to keep teaching, learning, and assessment running safely through disruption. Within this framing, cybersecurity awareness is one human-level input among several (alongside governance, training, and organisational culture) that jointly determine an institution's digital learning resilience.

These developments collectively suggest that conventional cybersecurity awareness — centred on passwords, email hygiene, and software updates — while still a necessary foundation for digital learning

resilience, is unlikely to be sufficient on its own for institutions operating AI-enabled digital ecosystems. This is a proposition this paper returns to in the Discussion and Implications sections, framed explicitly as an interpretation of the literature rather than a claim tested by the present data.

2.4 Responsible AI in Higher Education

International frameworks increasingly call for AI systems in education to be human-centred, transparent, accountable, secure, and privacy-preserving. UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021) and the OECD AI Principles both emphasise trustworthy, secure AI that protects learners' rights (OECD, 2024), while the NIST AI Risk Management Framework and ISO/IEC 42001 provide organisational mechanisms for managing AI-related risk, including security and resilience, throughout the AI lifecycle (NIST, 2024). Selwyn (2019) frames responsible AI adoption in education as fundamentally a question of values and governance rather than a purely technical exercise, a view echoed in Williamson's (2017) call for educators, not only technologists, to shape how data-driven systems are designed and used in schools and universities. Within Kuwait, national cybersecurity and digital transformation strategies have so far focused predominantly on technical infrastructure and general compliance, with comparatively little attention to AI-specific governance in higher education — a gap that mirrors the empirical gap this study addresses at the level of cybersecurity awareness.

2.5 AI Literacy and Student Digital Competence

AI literacy — the capacity to understand, critically evaluate, and use AI tools appropriately — has emerged as a distinct competence alongside conventional digital literacy (Long & Magerko, 2020; UNESCO, 2023). For students, AI literacy increasingly includes an element of digital self-protection: understanding what happens to coursework, personal data, or draft assessments entered into public generative AI tools, and recognising when an AI-generated communication (such as a phishing email or an academic-integrity trap) may not be what it appears to be. For academic staff, parallel competencies include the ability to design AI-aware assessment, to model safe and transparent AI use, and to protect student data when integrating AI tools into teaching. Zawacki-Richter et al. (2024) and Ifenthaler and Schumacher (2023) both note that institutional support for these competencies remains uneven, with cybersecurity awareness training and AI literacy development typically delivered — where they exist at all — as separate, uncoordinated initiatives rather than as a single, coherent programme of digital competence for AI-enabled learning.

2.6 Synthesis and Research Gap

Four observations emerge from this review. First, cybersecurity within GCC higher education remains understudied relative to more general digital transformation research. Second, existing cybersecurity awareness research rarely engages explicitly with the AI-enabled teaching and learning context in which universities now operate, even though that context plausibly changes what 'adequate' awareness looks like for both staff and students. Third, learning analytics and AI-in-education research has, as Williamson (2017) and Ifenthaler and Schumacher (2023) both suggest, given far more attention to pedagogical and predictive value than to the security and governance foundations that make that value trustworthy.

Fourth, no published study known to the authors has tested how conventional cybersecurity knowledge, threat awareness, and practices relate to one another within a Kuwaiti higher education sample specifically. This study addresses the fourth gap directly, through the empirical analysis reported in Sections 5–6, and addresses the first three gaps at the level of literature synthesis and conceptual discussion, clearly distinguishing that discussion from the tested empirical model.

3. Theoretical Framework

This study draws on three complementary behavioural and organisational theories to explain the relationships tested empirically, and to situate the discussion of AI-enabled learning environments that follows in later sections.

3.1 Protection Motivation Theory

Protection Motivation Theory (PMT; Rogers, 1975) proposes that individuals adopt protective behaviours after appraising the severity of a threat, their vulnerability to it, the efficacy of available responses, and their own capability to enact them (self-efficacy). Applied to cybersecurity in an educational setting, PMT predicts that students and staff who understand cyber threats and believe they can respond to them effectively are more likely to adopt secure practices when using digital learning platforms, learning analytics dashboards, and AI-enabled tools. PMT provides the primary theoretical rationale for this study's central hypothesis: that cybersecurity knowledge and cyber threat knowledge should predict cybersecurity practices.

3.2 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB; Ajzen, 1991) explains how intentions translate into behaviour through attitudes, subjective norms, and perceived behavioural control. Within universities, students' and staff's willingness to follow cybersecurity guidance is shaped not only by what they know but by institutional norms — including whether academic staff visibly model secure practice — and by whether they feel capable of managing digital risks, for example, whether they have received adequate training or have access to technical support. TPB is discussed here as a complementary lens for interpreting why knowledge alone may not fully translate into consistent practice, a pattern this study's descriptive findings touch on and one with direct implications for how staff development and student induction are designed.

3.3 Socio-Technical Systems Theory

Socio-Technical Systems Theory (STS; Baxter & Sommerville, 2011) holds that organisational performance depends on the joint optimisation of social and technical systems rather than either alone. Cybersecurity incidents rarely result purely from technological weakness; they typically arise from interactions between technology, governance, culture, and human behaviour. Applied to a university, this means that curriculum design, staff development, student induction, and technical controls need to be treated as a single system rather than addressed in isolation. This perspective supports the paper's

broader argument, developed in the Implications section, that university cybersecurity strategies — particularly as institutions adopt AI — need to combine technical safeguards with sustained investment in human capability, rather than treating either in isolation.

3.4 Application to This Study

Together, these three theories justify treating cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices as an interrelated behavioural system worth testing empirically (PMT and TPB), while also cautioning against interpreting individual awareness in isolation from institutional and pedagogical context (STS). Concepts such as AI literacy, responsible AI, and digital learning resilience, introduced in Sections 1 and 2, are treated in this paper as sensitising concepts that motivate and contextualise the study rather than as formally operationalised theoretical constructs, since the survey instrument used here was not designed to measure them. Section 4 makes this distinction explicit in the form of a conceptual model and a clearly delineated set of research propositions for future work.

4. Conceptual Framework and Hypothesis

4.1 The Empirical Model

Guided by Protection Motivation Theory (PMT) and supported by the complementary perspectives of the Theory of Planned Behaviour (TPB) and Socio-Technical Systems Theory (STS), this study examines the relationships between cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices among students and staff in Kuwait's higher education institutions. These constructs were selected because they represent the core dimensions of cybersecurity awareness measured by the survey instrument and provide the basis for testing the study's central research question.

The empirical model proposes that both cybersecurity knowledge and cyber threat knowledge positively influence cybersecurity practices. Individuals with greater understanding of cybersecurity concepts and stronger awareness of cyber threats are expected to demonstrate more secure digital behaviours when interacting with institutional digital systems and online learning environments.

The empirical model is illustrated below:

Cybersecurity Knowledge → Cybersecurity Practices

Cyber Threat Knowledge → Cybersecurity Practices

Based on this model, the following hypothesis is tested:

H1: *Cybersecurity knowledge and cyber threat knowledge are significant positive predictors of cybersecurity practices among students and staff in Kuwait's higher education institutions.*

To provide a more rigorous assessment of these relationships, the ordinal logistic regression model additionally included demographic characteristics (age, gender, institutional role, field of study,

institution, and year of study) as control variables. Their inclusion allowed the study to determine whether the relationships between cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices remained significant after accounting for differences in participant characteristics.

4.2 An Educational Conceptual Extension for Future Research

While the empirical model focuses on the direct relationships between cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices, contemporary higher education increasingly operates within AI-enabled digital ecosystems in which cybersecurity forms only one component of a broader educational environment. Accordingly, this paper proposes an educational conceptual framework that situates the empirical findings within the wider context of AI-enabled teaching and learning.

The framework presented in Fig. 1 positions cybersecurity awareness as a foundational capability supporting secure digital behaviour, which in turn contributes to trust in digital technologies, digital learning resilience, and ultimately educational quality. Rather than viewing cybersecurity solely as a technical or administrative function, the framework conceptualises it as an educational capability that enables the responsible adoption of learning analytics, generative AI, and other AI-supported learning technologies.

Specifically, the framework proposes that AI-enabled teaching and learning generates increasing reliance on learning analytics and responsible AI practices. These developments require students and staff to demonstrate appropriate cybersecurity awareness and secure digital behaviours. Secure behaviours strengthen trust in digital learning environments, support institutional digital resilience, and create conditions in which AI technologies can be implemented safely, ethically, and effectively to enhance educational quality.

Importantly, the conceptual framework extends rather than replaces the empirical model tested in this study. The empirical analysis provides evidence that cybersecurity knowledge and cyber threat knowledge significantly predict cybersecurity practices. Building on these findings, the framework offers a broader educational perspective by illustrating how secure digital behaviour may contribute to trustworthy AI-enabled learning environments. It therefore serves as a theoretical foundation for future studies examining AI literacy, learning analytics governance, responsible AI, digital trust, and digital learning resilience using more comprehensive research designs, including structural equation modelling.

5. Methodology

5.1 Research Design

This study employed a quantitative, cross-sectional survey design to examine the relationships between cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices among students and staff in higher education institutions in Kuwait. A quantitative survey was considered appropriate because it

enabled the collection of standardised data from a relatively large sample and facilitated statistical examination of the relationships between the study variables. Although cross-sectional designs do not permit causal inference or the assessment of change over time, they provide an effective approach for evaluating cybersecurity awareness during a period of rapid digital and AI-enabled transformation in higher education.

5.2 Research Context

The study was conducted within Kuwait's higher education sector, which has experienced accelerated digital transformation following the COVID-19 pandemic and in line with the objectives of Kuwait Vision 2035. Universities have increasingly adopted cloud-based learning management systems, digital assessment platforms, online communication technologies, and, more recently, AI-enabled educational tools. These developments have expanded the collection and use of educational data, increasing the importance of cybersecurity awareness for protecting digital learning environments, safeguarding sensitive information, and supporting trustworthy AI-enabled education.

5.3 Participants and Sampling

Data were collected through an online questionnaire distributed between October and December 2025 to students and staff across seven higher education institutions in Kuwait. A convenience sampling strategy was adopted because it enabled broad institutional participation within the practical constraints of the study.

A total of 274 questionnaires were returned. Following data screening, four incomplete or inconsistent responses were excluded, resulting in a final sample of 270 participants. Students represented approximately 88% of respondents, while staff accounted for the remaining 12%. The sample was predominantly female (approximately 86%), and most participants were aged between 18 and 24 years (Fig. 2). Although these characteristics broadly reflect the participating institutions, they may limit the generalisability of the findings beyond similar higher education contexts.

5.4 Research Instrument

Data were collected using a structured questionnaire comprising four sections and 15 items measured on five-point Likert scales. The first section collected demographic information, including age, gender, institutional role, and field of study. The remaining sections measured the study's three constructs:

- **Cybersecurity Knowledge** – understanding of cybersecurity concepts, institutional security policies, and cybersecurity training;
- **Cyber Threat Knowledge** – awareness of common cyber threats, including phishing, malware, ransomware, password attacks, and social engineering; and
- **Cybersecurity Practices** – routine security behaviours, including password management, software updating, and antivirus use.

The questionnaire was reviewed by subject specialists to establish content validity and was pilot-tested to assess clarity, readability, and completion time before full administration. The instrument was designed to measure conventional cybersecurity awareness and therefore focused on established cybersecurity constructs rather than AI-specific competencies.

This study was conducted in accordance with the ethical principles of the Declaration of Helsinki and the PAAET institutional ethical guidelines governing research involving human participants. Informed consent was obtained from all participants prior to participation in the study. Participants were informed about the purpose of the research, that participation was voluntary, that responses would remain anonymous and confidential, and that they could withdraw at any time without consequence.

5.5 Reliability

Internal consistency was assessed using Cronbach's alpha across the 15 items comprising the three constructs. The overall questionnaire achieved α = .870 (standardised-items α = .869). Individual constructs also exceeded the conventional .70 threshold: Cybersecurity Knowledge (α = .724), Cyber Threat Knowledge (α = .827), and Cybersecurity Practices (α = .764), indicating satisfactory reliability for research purposes.

Table 1
Overall reliability of the measurement instrument.

Reliability statistic	Value
Cronbach's Alpha	.870
Cronbach's Alpha Based on Standardized Items	.869
N of Items	15

Table 1
a. Reliability by construct.

Construct	Cronbach's α	Interpretation
Cybersecurity Knowledge	.724	Acceptable
Cyber Threat Knowledge	.827	Good
Cybersecurity Practices	.764	Acceptable

5.6 Analytical Approach

Data were screened, cleaned, and analysed using IBM SPSS Statistics version 29. The Kolmogorov–Smirnov and Shapiro–Wilk tests indicated significant departures from normality across all three constructs (Table 2). Consequently, non-parametric statistical techniques were employed throughout the analysis.

Spearman's rank-order correlation was used to examine the relationships between cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices. Ordinal logistic regression was subsequently employed to test the study's hypothesis by determining whether cybersecurity knowledge and cyber threat knowledge significantly predicted cybersecurity practices while controlling for demographic characteristics. Additional Mann–Whitney U and Kruskal–Wallis tests were conducted to explore potential differences across demographic groups. These subgroup analyses were exploratory and were undertaken to provide additional context for interpreting the main findings.

Table 2
Tests of normality (Lilliefors significance correction).

Construct	Kolmogorov-Smirnov Statistic	df	Sig.	Shapiro-Wilk Statistic	df	Sig.
Cybersecurity Knowledge	.101	269	< .001	.983	269	.002
Cyber Threat Knowledge	.073	269	.001	.976	269	< .001
Cybersecurity Practices	.058	269	.029	.981	269	.001

6. Data Analysis and Results

6.1 Descriptive Overview

Table 3 reports descriptive statistics for the three study constructs. On the five-point scale used throughout the instrument, respondents reported moderate mean levels of Cybersecurity Knowledge (M = 2.87, SD = 0.85), Cyber Threat Knowledge (M = 2.83, SD = 1.03), and Cybersecurity Practices (M = 3.00, SD = 1.00), with all three constructs showing considerable spread (ranges of 3.80–4.00 points) and only modest skewness and kurtosis. These patterns indicate a population clustered around the midpoint of the scale — neither strongly confident nor strongly lacking in cybersecurity knowledge and practice — with meaningful variation across individuals rather than a ceiling or floor effect.

Statistic	Cybersecurity Knowledge	Cyber Threat Knowledge	Cybersecurity Practices
Mean (SE)	2.868 (.052)	2.832 (.063)	2.999 (.061)
95% CI for Mean	[2.766, 2.971]	[2.709, 2.956]	[2.879, 3.120]
Median	3.000	2.800	3.000
SD	.853	1.029	1.004
Variance	.728	1.059	1.007
Minimum	1.00	1.00	1.00
Maximum	4.80	5.00	5.00
Range	3.80	4.00	4.00
Interquartile range	1.20	1.60	1.35
Skewness (SE = .149)	-.194	.113	-.044
Kurtosis (SE = .296)	-.509	-.674	-.575

Table 3. Descriptive statistics for study variables (N = 269–270).

Figures 4 and 5 illustrate two items underlying these constructs: respondents' self-reported familiarity with the term "cybersecurity", and their prior participation in formal cybersecurity education or training. Consistent with the moderate mean scores in Table 3, responses to both items were mixed rather than uniformly high or low, and a substantial proportion of respondents reported no prior formal cybersecurity training. This pattern is consistent with the paper's broader argument that formal cybersecurity training is not yet reaching all students and staff consistently, and that knowledge does not automatically translate into consistent practice, with direct implications for how safely this population is likely to engage with AI-enabled learning tools.

6.2 Correlation Analysis

Spearman's rank-order correlation was used to examine the relationships between Cybersecurity Knowledge (CK), Cyber Threat Knowledge (CTK), and Cybersecurity Practices (CP), given the non-normal distribution of the data.

Variable	CK	CTK	CP
Cybersecurity Knowledge (CK)	1.000	.543**	.422**
Cyber Threat Knowledge (CTK)	.543**	1.000	.420**
Cybersecurity Practices (CP)	.422**	.420**	1.000

*Table 4. Spearman correlations between study variables (N = 269–270). **p < .001.*

All three constructs were significantly and positively correlated. Cybersecurity Knowledge and Cyber Threat Knowledge showed a moderate-to-strong positive association (ρ = .543, p < .001), suggesting that participants with stronger foundational cybersecurity understanding also tended to be more familiar with specific cyber threats. Both Cybersecurity Knowledge (ρ = .422, p < .001) and Cyber Threat Knowledge (ρ = .420, p < .001) were moderately and positively associated with Cybersecurity Practices, indicating that greater knowledge and threat awareness were both associated with more secure day-to-day digital behaviour, consistent with Protection Motivation Theory.

6.3 Ordinal Logistic Regression

An ordinal logistic regression model was estimated with Cybersecurity Practices as the ordinal dependent variable, Cybersecurity Knowledge and Cyber Threat Knowledge entered as the primary predictors to test H1, and age, gender, institutional role, field of study, institution, and year of study entered as covariates.

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	1365.981	—	—	—
Final	804.864	561.117	750	1.000

Goodness-of-Fit	Chi-Square	df	Sig.
Pearson	114617.734	5700	<.001
Deviance	797.932	5700	1.000

Table 5. Model fitting information and goodness-of-fit.

Pseudo R-Square	Value
Cox and Snell	.918
Nagelkerke	.920
McFadden	.409

Table 6. Pseudo R-square.

The model fit statistics presented in Tables 5 and 6 should be interpreted in the context of the complexity of the fitted model. The inclusion of six multi-level categorical covariates together with the two focal predictors resulted in a large number of estimated parameters relative to the sample size (N =

270). Consequently, the model produced very high pseudo-R^2 values and some divergence between the Pearson and Deviance goodness-of-fit statistics, while the SPSS output reported Hessian-matrix singularities for several demographic covariates. These patterns are consistent with sparse data across some covariate categories and primarily affect the estimation of the demographic control variables rather than the substantive predictors. Importantly, the parameter estimates for the two focal constructs —Cybersecurity Knowledge and Cyber Threat Knowledge—were stable, with reasonable standard errors, narrow confidence intervals, and statistically significant effects. As these variables represent the direct test of H1, the findings provide robust evidence that both cybersecurity knowledge and cyber threat knowledge are significant predictors of cybersecurity practices after accounting for demographic characteristics.

Effect	-2LL of Reduced Model	Chi-Square	df	Sig.
Cybersecurity Knowledge	866.351	61.487	30	<.001
Cyber Threat Knowledge	867.043	62.179	30	<.001
Age	6221.451	5416.587	150	<.001
Gender	859.671	54.807	30	.004
Role at the university	796.078	—	30	—
Field of study / department	856.485	51.621	150	1.000
University	828.914	24.050	180	1.000
Year of study	917.045	112.181	150	.991

Table 7. Likelihood ratio tests for model effects. The likelihood ratio tests indicate that Cybersecurity Knowledge and Cyber Threat Knowledge made significant independent contributions to the model. Interpretation of several demographic covariates should be made with appropriate caution because sparse observations across some multi-level categories resulted in Hessian-matrix singularities in the SPSS estimation procedure. These estimation characteristics primarily affect selected control variables and do not alter the significance or interpretation of the study's focal predictors.

Table 8 reports the key location-parameter estimates for the two predictors that directly test H1. Both were statistically significant, independent, positive predictors of Cybersecurity Practices: Cybersecurity Knowledge (B = .943, SE = .186, Wald = 25.695, df = 1, p < .001, 95% CI [.578, 1.307]) and Cyber Threat Knowledge (B = .520, SE = .149, Wald = 12.227, df = 1, p < .001, 95% CI [.228, .811]). Participants with greater cybersecurity knowledge and greater cyber threat knowledge were significantly more likely to report higher levels of secure digital practice, supporting H1. Among the demographic covariates, only a small number of individual category comparisons reached significance at the .05 level, and — consistent

with the caution above — these should be treated as exploratory given the model specification issues noted in Table 7.

Predictor	B	Std. Error	Wald	df	Sig.	95% CI Lower	95% CI Upper
Cybersecurity Knowledge	.943	.186	25.695	1	<.001	.578	1.307
Cyber Threat Knowledge	.520	.149	12.227	1	<.001	.228	.811

Table 8. Ordinal logistic regression location-parameter estimates for the focal predictors of H1 (link function: logit). Full parameter estimates including demographic covariates and threshold values are available from the authors on request.

6.4 Exploratory Subgroup Comparisons

Beyond the pre-specified hypothesis, exploratory non-parametric tests examined whether the three constructs varied by gender, institutional role, and age group. These comparisons were not part of H1 and are reported for completeness and to inform the practical recommendations in Section 8.

Independent-samples Mann-Whitney U tests indicated statistically significant gender differences on all three constructs: Cybersecurity Knowledge ($p = .042$), Cyber Threat Knowledge ($p = .034$), and Cybersecurity Practices ($p = .002$, Mann-Whitney $U = 5183.000$, $N = 269$).

Test	Cybersecurity Knowledge	Cyber Threat Knowledge	Cybersecurity Practices
Asymptotic Sig. (gender)	.042	.034	.002
Decision	Reject null	Reject null	Reject null

Table 9. Mann-Whitney U test results by gender (distribution equality across gender categories).

A Kruskal-Wallis H test found no statistically significant differences across the six age bands for any of the three constructs (Cybersecurity Knowledge: $H = 8.582$, $df = 5$, $p = .127$; Cyber Threat Knowledge: $H = 5.050$, $df = 5$, $p = .410$; Cybersecurity Practices: $H = 6.557$, $df = 5$, $p = .256$), suggesting that, unlike gender, age was not associated with meaningful differences in this sample.

A further Mann-Whitney U test comparing students and staff (role at the university) found no significant difference in Cybersecurity Knowledge ($p = .591$) or Cyber Threat Knowledge ($p = .461$), but a significant difference in Cybersecurity Practices ($p = .040$), indicating that while students and staff reported broadly similar levels of knowledge, their routine security behaviours differed.

Comparison	Cybersecurity Knowledge Sig.	Cyber Threat Knowledge Sig.	Cybersecurity Practices Sig.
Role at the university (student vs staff)	.591	.461	.040

Table 10. Mann-Whitney U test results by role at the university.

Taken together, these exploratory comparisons suggest that gender and role, but not age, are associated with meaningful variation in this sample's cybersecurity profile — a pattern returned to in Section 7 and Section 8 when discussing who cybersecurity and AI-literacy training should prioritise.

7. Discussion

7.1 Knowledge and Threat Awareness Predict Secure Practice

Finding. The findings support the study's central hypothesis: cybersecurity knowledge and cyber threat knowledge are meaningfully and positively related to cybersecurity practices among staff and students in Kuwaiti higher education institutions, both in bivariate correlation (Section 6.2) and in the ordinal logistic regression controlling for demographic covariates (Section 6.3).

Comparison with previous studies. This is consistent with Protection Motivation Theory's prediction that threat appraisal and perceived capability jointly motivate protective behaviour, and it echoes prior cybersecurity awareness research conducted in other national contexts (Ifinedo, 2012; Kruger & Kearney, 2006).

Educational meaning. For a higher education population, this relationship matters beyond information-security compliance: it indicates that where cybersecurity knowledge is built — through curriculum, induction, or training — secure behaviour tends to follow. Knowledge, in other words, is an educational lever available to institutions, not only a risk-management input.

Implications for AI-enabled learning. If foundational knowledge shapes secure behaviour around relatively familiar threats, it plausibly also shapes how safely students and staff engage with AI-enabled tools — for example, whether a student recognises that pasting an assessment brief into an unfamiliar generative AI tool carries a data-handling risk, or whether a lecturer verifies an AI-generated communication before acting on it.

Implications for universities. Institutions should treat cybersecurity knowledge-building as part of digital and AI literacy development, not a separate compliance exercise delivered in isolation from teaching and learning.

7.2 Knowledge Does Not Fully Determine Practice

Finding. The moderate — rather than strong — size of the correlations, together with the descriptive evidence in Section 6.1 showing considerable spread and a substantial proportion of respondents without formal training, suggests that knowledge alone does not fully determine behaviour.

Comparison with previous studies. This is consistent with the Theory of Planned Behaviour's emphasis on norms and perceived behavioural control: even well-informed individuals may not act securely if institutional support, training, or organisational culture do not reinforce secure practice. Socio-Technical Systems Theory offers a complementary reading — that cybersecurity outcomes emerge from the interaction of technical systems, governance, and human behaviour rather than from individual knowledge in isolation.

Educational meaning. This gap between knowing and doing is a familiar pattern in educational research more broadly, and it suggests that cybersecurity awareness should be taught and reinforced the way other applied competencies are: through modelling, practice, and feedback, not one-off instruction. The exploratory finding that students and staff reported similar knowledge but significantly different practices (Section 6.4, Table 10) reinforces this point directly: it is unlikely to be a knowledge gap between the two groups so much as a difference in routine, workflow, or institutional expectation.

Implications for AI-enabled learning. As AI tools become embedded in coursework, the gap between knowing and doing may widen further, since AI-specific risks are, by design, harder to recognise as risks than conventional phishing or malware.

Implications for universities. Universities should pair knowledge-building with visible institutional reinforcement — clear policy, staff modelling of secure practice, and low-friction technical support — rather than assuming that training alone will change behaviour. The significant gender differences observed across all three constructs (Section 6.4, Table 9) also suggest that training and communication strategies may need to be designed and evaluated with attention to whether they reach all groups equally, rather than assuming a single approach works uniformly across a diverse student and staff population.

7.3 A Cautious Extension to AI-Enabled Risk

Finding. These results also speak, cautiously, to the wider concern motivating this paper.

Comparison with previous studies. If conventional cybersecurity knowledge only moderately predicts secure practice under relatively familiar threat conditions (phishing, malware, password attacks), the literature on AI-specific threats (World Economic Forum, 2025; NIST, 2024) suggests these will place additional demands on awareness.

Educational meaning. AI-specific threats are by design harder to recognise as threats at all — a persuasive AI-generated phishing email, or an academic-integrity trap embedded in an AI tool's output, does not announce itself the way a poorly spelled scam email once did.

Implications for AI-enabled learning. Current instruments and training programmes, including the one measured here, are not yet designed to capture or address these AI-specific dimensions of awareness.

Implications for universities. This is offered as an interpretation to be tested in future research, not as a finding of the present study, which did not measure AI-specific threat recognition directly; it nonetheless points toward the practical recommendations developed in Section 8.

8. Practical and Policy Implications

8.1 Strengthening Conventional Cybersecurity Awareness

The immediate, evidence-based implication of this study is that Kuwaiti HEIs should strengthen conventional cybersecurity training, given the moderate knowledge levels and inconsistent practices observed, and the substantial proportion of respondents reporting no prior formal training (Section 6.1, Fig. 5). This includes regular, mandatory training (rather than one-off sessions), clearer institutional security policies, and periodic phishing-recognition exercises for both students and staff.

8.2 Implications for Academic Staff

Building on the literature discussed in Sections 1–3, and offered here as a forward-looking recommendation rather than a data-driven finding, academic staff who integrate AI tools into teaching should be supported to develop: AI security awareness appropriate to their teaching role; secure assessment design practices that anticipate AI-related integrity risks; safe handling and protection of student data when using AI or learning analytics tools; responsible, transparent AI use that is modelled openly to students; and safe-prompting practices that avoid entering sensitive student or institutional data into public generative AI tools.

8.3 Implications for Students

Students likewise need support to develop: AI literacy that includes an understanding of what happens to data entered into generative AI tools; digital citizenship and cyber hygiene appropriate to a data-intensive learning environment; the ability to recognise AI-enabled social engineering and academic-integrity traps; and an understanding of how to protect their own personal and academic data across the platforms they use for learning.

8.4 Learning Analytics Governance

As learning analytics use grows, institutions should establish clear governance around data ownership, informed consent, retention, and transparency — independent of whether AI is directly involved — so that any future expansion toward AI-enhanced analytics builds on a sound data-governance foundation rather than retrofitting one.

8.5 Institutional Recommendations

Table 11
summarises institutional-level recommendations arising from this study, organised by area of action.

Area	Recommendation
Curriculum	Embed cybersecurity and AI literacy explicitly within digital literacy curricula, rather than treating them as separate, optional add-ons
Staff development	Provide regular, mandatory cybersecurity and responsible-AI training for academic staff, tied to how AI tools are used in their own teaching
Student induction	Introduce mandatory cybersecurity and AI-literacy induction for new students, reinforced periodically rather than delivered once
Learning analytics	Establish ethical governance structures covering data ownership, consent, retention, and transparency
AI use	Develop and communicate an institutional responsible-AI policy covering teaching, assessment, and administrative use
Assessment	Update academic-integrity policy and practice to be AI-aware, addressing both misuse of AI and AI-enabled deception
Data protection	Adopt a clear privacy framework covering student and staff data collected through learning platforms and AI tools
Targeting	Design training and communication with attention to subgroup differences (Section 6.4) — for example, the observed gender differences in practices, and the difference in practices, though not knowledge, between students and staff

Table 11. *Institutional recommendations for cybersecurity awareness in AI-enabled higher education.*

8.6 Policy Implications for Kuwait

These findings are relevant to the human-capability objectives of Kuwait's National Cybersecurity Strategy and to the digital transformation goals of Kuwait Vision 2035. Policymakers and institutional leaders may wish to consider: mandating baseline cybersecurity and AI-literacy training across HEIs; developing shared, sector-wide awareness resources rather than requiring each institution to build these independently; and — as AI adoption grows — commissioning dedicated research (of the kind proposed in Section 4.2) to measure AI literacy, learning analytics governance maturity, and AI-specific threat awareness directly, rather than assuming these track conventional cybersecurity awareness.

9. Contributions

This study makes five specific contributions. First, it provides empirical evidence on cybersecurity knowledge, threat knowledge, and practices from an underrepresented regional and educational context — Kuwait's higher education sector — using a reliable instrument ($\alpha = .870$) and a statistically tested model linking these constructs, including confirmation via ordinal logistic regression that the relationships hold after accounting for demographic composition. Second, it integrates cybersecurity awareness research with the AI-in-education and learning analytics literatures, a combination that has so

far developed largely in isolation. Third, it extends Protection Motivation Theory, the Theory of Planned Behaviour, and Socio-Technical Systems Theory into the context of AI-supported higher education, showing how these established behavioural frameworks can inform, rather than be displaced by, the study of AI-enabled risk. Fourth, it proposes an educational conceptual framework (Section 4.2) — positioning cybersecurity awareness as one link between AI-enabled teaching and learning and educational quality — together with a concrete agenda for the instrument development and data collection that testing this framework would require. Fifth, it offers practical guidance for universities implementing AI, distinguishing explicitly between recommendations grounded in the present data and forward-looking recommendations offered for discussion.

10. Limitations and Future Research

Several limitations should be acknowledged. First, the cross-sectional design precludes causal inference; longitudinal studies would provide greater insight into how cybersecurity awareness and secure digital practices evolve as AI-enabled technologies become increasingly embedded within higher education. Second, the use of convenience sampling across seven Kuwaiti higher education institutions, together with the predominance of younger and female respondents, limits the generalisability of the findings to other institutional settings, demographic groups, and national contexts. Third, the ordinal logistic regression model reported in Section 6.3 included six demographic covariates in addition to the two focal predictors, resulting in a relatively complex model for the available sample size. Consequently, sparse observations across some demographic categories produced Hessian-matrix singularities and influenced the stability of selected covariate estimates. Importantly, these estimation characteristics primarily affected the demographic control variables and did not alter the statistical significance or interpretation of the two focal predictors used to test H1. Finally, the survey instrument measured conventional cybersecurity constructs only and did not directly assess AI literacy, learning analytics awareness, AI governance, or digital learning resilience. Accordingly, the broader educational implications discussed in this paper should be interpreted as a conceptual extension of the empirical findings rather than as relationships tested directly by the survey.

Future research should directly examine the constructs proposed in Section 4.2—including AI literacy, learning analytics awareness, AI governance maturity, digital trust, and digital learning resilience—using validated measurement instruments. Structural equation modelling would enable simultaneous testing of the broader conceptual framework proposed in this study. Future studies could also evaluate the effectiveness of integrated cybersecurity and AI-literacy interventions, employ mixed-methods approaches combining surveys with interviews or classroom observations, undertake longitudinal investigations of AI adoption within higher education, and conduct comparative research across GCC countries to determine whether the relationships identified in this study, including the observed gender and institutional-role differences, are consistent across different educational and cultural contexts.

11. Conclusion

This study examined the relationships between cybersecurity knowledge, cyber threat knowledge, and cybersecurity practices among 270 staff and students across seven higher education institutions in Kuwait. The findings show that cybersecurity knowledge and threat knowledge are significantly and positively associated with secure digital practice — confirmed through both correlation and ordinal logistic regression — while also revealing gaps in training and inconsistencies between knowledge and behaviour that warrant institutional attention, particularly as these gaps carry over into how safely students and staff engage with AI-enabled learning tools.

The paper has also situated these findings within the wider, evolving landscape of AI-enabled higher education, arguing that conventional cybersecurity awareness — while a necessary foundation — is unlikely on its own to prepare students and staff for the AI-specific risks that increasingly accompany AI adoption in teaching and learning. This argument has been presented consistently as a conceptual contribution motivating future research, not as a claim tested by the present data, and the paper has aimed throughout to keep that distinction clear for readers and reviewers alike. Strengthening conventional cybersecurity awareness now — embedded within, rather than separate from, digital and AI literacy development for staff and students — while building the instruments needed to measure AI-specific readiness directly, offers a realistic and honest path toward more digitally resilient, and more trustworthy, AI-enabled higher education in Kuwait and comparable contexts.

Declarations

Conflict of interest.

The author declares no conflict of interest.

Ethics approval and Consent to Participate:

Ethical approval was obtained from the Research Ethics Committee of the Public Authority for Applied Education and Training (PAAET), Kuwait. The study was conducted in accordance with the Declaration of Helsinki and PAAET's ethical guidelines. Informed consent was obtained from all participants before participation.

Consent to Publish:

Informed consent for publication of anonymised research findings was obtained from all participants.

Clinical Trial Number

Not applicable.

Funding.

This research received no external funding

Author Contribution

One author, AFA wrote and reviewed the article

Data Availability

Data available on request from author

References

1. Ajzen I. The theory of planned behavior. Organ Behav Hum Decis Process. 1991;50(2):179–211.
2. Baxter G, Sommerville I. Socio-technical systems: From design methods to systems engineering. Interact Comput. 2011;23(1):4–17.
3. Crompton H, Burke D. Artificial intelligence in higher education: The state of the field. Computers Education: Artif Intell. 2024;7:100292.
4. ENISA. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity; 2024.
5. Holmes W, Bialik M, Fadel C. Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. 2nd ed. Center for Curriculum Redesign; 2022.
6. IBM Security. Cost of a Data Breach Report 2024. IBM Corporation; 2024.
7. Ifenthaler D, Schumacher C. Student perceptions of privacy principles for learning analytics. Education Tech Research Dev. 2023;71(1):63–86.
8. Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers Security. 2012;31(1):83–95.
9. Kasneci E, Sessler K, Küchemann S, Bannert M, Dementieva D, Fischer F, Gasser U, Groh G, Günnemann S, Hüllermeier E, Krusche S, Kutyniok G, Michaeli T, Nerdel C, Pfeiffer F, Poquet O, Sailer M, Schmidt A, Seidel T, Kasneci G. ChatGPT for good? On opportunities and challenges of large language models for education. Learn Individual Differences. 2023;103:102274.
10. Kruger HA, Kearney WD. A prototype for assessing information security awareness. Computers Security. 2006;25(4):289–96.
11. Long D, Magerko B. (2020). What is AI literacy? Competencies and design considerations. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–16). ACM.
12. Luckin R, Holmes W, Griffiths M, Forcier LB. Intelligence Unleashed: An Argument for AI in Education. Pearson; 2016.
13. National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0): Generative AI Profile. U.S. Department of Commerce; 2024.

14. OECD. OECD Framework for the Classification of AI Systems. Organisation for Economic Co-operation and Development; 2024.
15. Rogers RW. A protection motivation theory of fear appeals and attitude change. J Psychol. 1975;91(1):93–114.
16. Selwyn N. Should Robots Replace Teachers? AI and the Future of Education. Polity; 2019.
17. Siemens G, Baker RSJ. d. (2012). Learning analytics and educational data mining: Towards communication and collaboration. In *Proceedings of the 2nd International Conference on Learning Analytics and Knowledge* (pp. 252–254). ACM.
18. UNESCO. Recommendation on the Ethics of Artificial Intelligence. UNESCO; 2021.
19. UNESCO. Guidance for Generative AI in Education and Research. UNESCO; 2023.
20. Williamson B. Big Data in Education: The Digital Future of Learning, Policy and Practice. SAGE; 2017.
21. World Economic Forum. Global Cybersecurity Outlook 2025. World Economic Forum; 2025.
22. Zawacki-Richter O, Bond M, Marin VI, Gouverneur F. Systematic review of artificial intelligence applications in higher education: Recent developments and future directions. Int J Educational Technol High Educ. 2024;21:1–29.

Figures

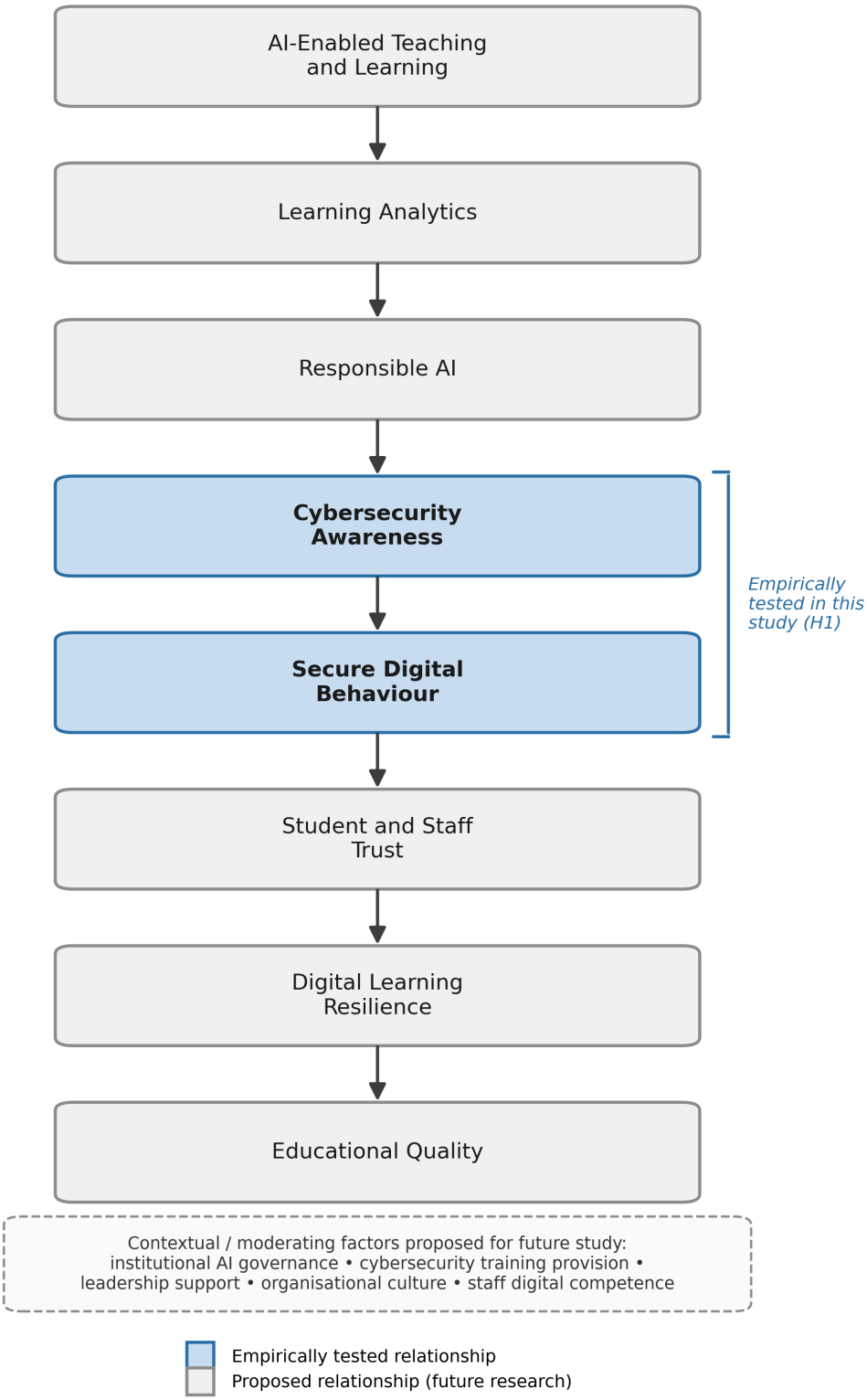


Figure 1

Educational conceptual framework linking AI-enabled teaching and learning, cybersecurity awareness, digital learning resilience, and educational quality. The shaded section represents the empirical relationships tested in this study, whereas the remaining pathways illustrate a conceptual framework to guide future research.

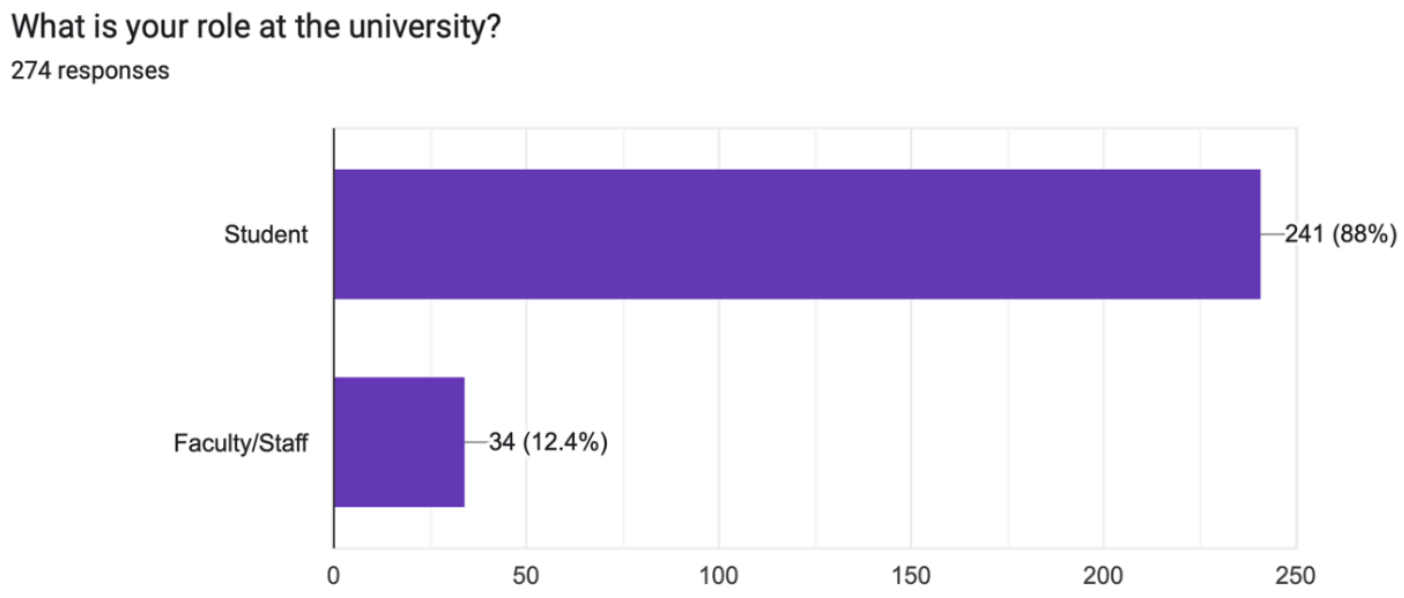


Figure 2

Distribution of respondents by role at the university (N = 274 responses, prior to data screening).

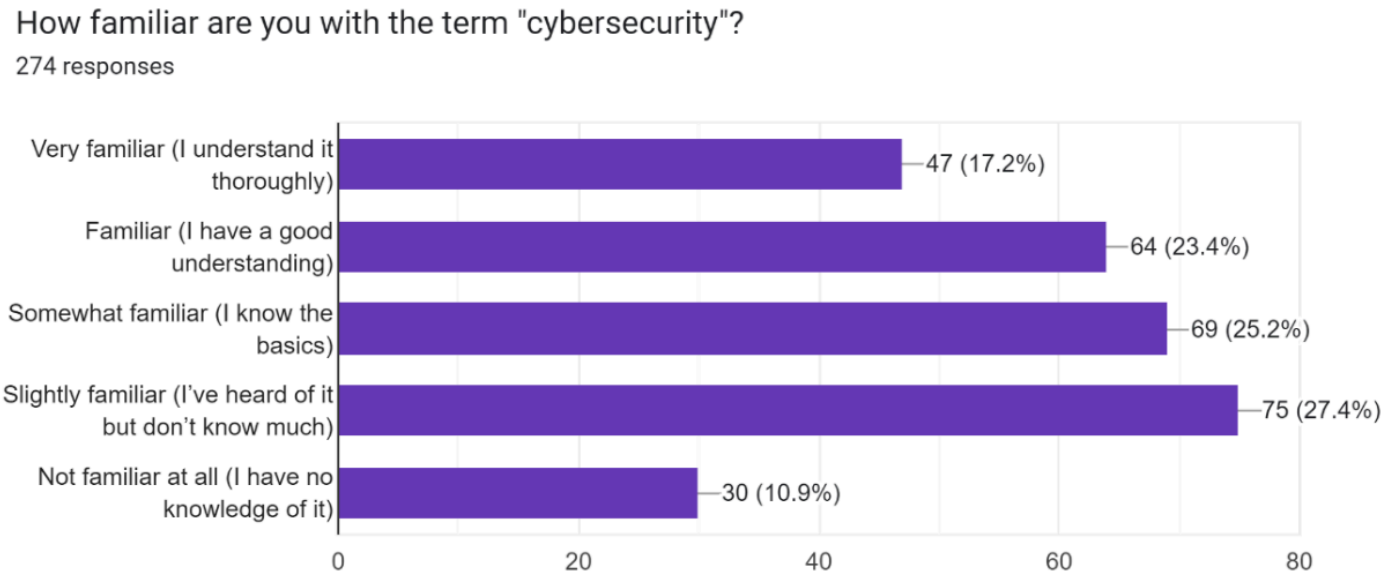


Figure 3

Respondents' self-reported familiarity with the term "cybersecurity" (N = 274 responses, prior to data screening).

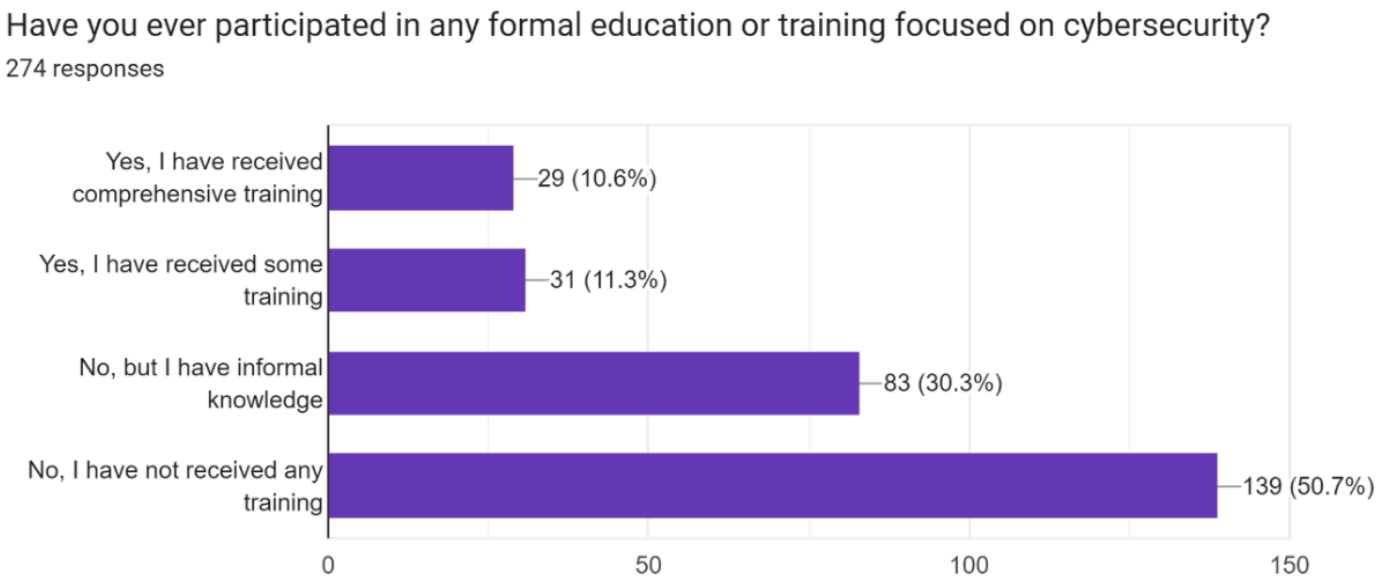


Figure 4

Respondents' prior participation in formal cybersecurity education or training (N = 274 responses, prior to data screening).