

**JOURNAL OF INFORMATION
SYSTEM AND TECHNOLOGY
MANAGEMENT
(JISTM)**www.gaexcellence.com/jistm**CYBERSECURITY AWARENESS IN EDUCATIONAL
INSTITUTIONS: A CRITICAL SOCIO-TECHNICAL
REVIEW OF BEHAVIOURAL, PEDAGOGICAL AND
GOVERNANCE INTERVENTIONS**

Nor Hafizah Abdul Razak¹, Siti Rafidah Muhamat Dawam^{2*}, Nurul Husna Mahadzir³,
Mazura Mat Din⁴, Shaifizat Mansor⁵

¹ Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kedah, Malaysia

 hafizah466@uitm.edu.my

 <https://orcid.org/0009-0004-4735-0435>

² Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kedah, Malaysia

 srafidah192@uitm.edu.my

 <https://orcid.org/0000-0002-6349-9406>

³ Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kedah, Malaysia

 husnamahadzir@uitm.edu.my

 <https://orcid.org/0000-0002-8607-5438>

⁴ Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kedah, Malaysia

 mazuramd@uitm.edu.my

 <https://orcid.org/0000-0002-9814-1316>

⁵ Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kedah, Malaysia

 shaifizat@uitm.edu.my

 <https://orcid.org/0009-0006-4781-1670>

*Corresponding Author

Article Info:**Article history:**

Received date: 30.07.2026

Revised date: 24.08.2026

Accepted date: 17.09.2026

Published date: 28.09.2026

To cite this document:

Razak, N. H. A., Muhamat Dawam, S. R., Mahadzir, N. H., Din, M. M., & Mansor, S. (2026). Cybersecurity Awareness in Educational Institutions: A Critical Socio-Technical Review of Behavioural, Pedagogical and

Abstract:

The increasing reliance on cloud services, learning management systems and connected devices has expended opportunities for teaching and learning within educational institutions. However, it also causes the risk of phishing, ransomware, data misuse and social engineering. So, this critical literature review examines cybersecurity awareness across primary, secondary and higher education from a socio-technical perspective. A structured search of academic research databases including Scopus, Web of Science, IEEE Xplore and ERIC, identified peer-reviewed studies published between 2021 and 2026. 15 studies have retained for thematic synthesis after duplicate elimination and staged screening. The analysis integrates Protection Motivation Theory (PMT) and Socio-Technical Systems (STS) theory to capture both individual and contextual influences on secure behaviour. PMT was used to interpret individual threat perception, coping appraisal and self-efficacy, while STS theory to examine how institutional and technological conditions influence secure behaviour. A persistent gap between recognizing cybersecurity risks and knowing how to respond

Governance Interventions.
*Journal of Information System
and Technology Management*,
11 (44), 572-588.

to the risk has been highlighted from the synthesis. Although, interactive and gamified interventions generally report improvements in short-term knowledge or awareness, the reviewed studies show that this evidence of sustained behavioural change remains limited. The reviewed studies also indicate that teacher capability, governance arrangements and institutional readiness influence whether cybersecurity knowledge is translated into practice. Across the literature, continuous assessment and role-specific training are presented more consistently as components of sustained cybersecurity practice than isolated awareness activities. These findings also question the adequacy of the “human firewall” metaphor, which places considerable responsibility on individual users while giving less attention to system design, governance and resource constraints. Cybersecurity awareness is therefore better understood in this review as an outcome of interactions among threat appraisal, self-efficacy, institutional support and secure system design.

DOI: 10.35631/JISTM.1144035 **Keyword:**

Cybersecurity Awareness, Educational Institutions, Protection Motivation Theory, Socio-Technical Systems, Digital Literacy, Cybersecurity Governance



© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact jistm@gaexcellence.com.

Introduction

Digital learning has changed the way educational institutions manage cybersecurity risk. Teaching, assessment and administration now depend heavily on learning management systems, cloud storage, mobile applications and connected classroom technologies. These systems improve access and efficiency, but they also increase the number of potential points of exposure and place large amounts of student and staff data across platforms managed by different internal and external parties. Recent studies in educational cybersecurity identify phishing, ransomware, credential theft, privacy breaches and third-party vulnerabilities as recurring concerns. At the same time, users do not always develop the knowledge or practical skills needed to respond to these risks at the same pace as technological change (Barbu et al., 2023; Malasowe et al., 2024).

Cybersecurity awareness is important; however, its effectiveness must be supported with technical controls and institutional governance. In educational settings, cybersecurity awareness extends beyond recognising common threats, including users' confidence, everyday practices and perceptions of risk. These cybersecurity awareness factors influence how students, teachers and administrators respond when they encounter security problems. The widely used concept of the “human firewall” highlights the role of user behaviour. However, placing too much responsibility on users' behaviour may overlook other factors that contribute

to security failures, such as weak access controls, insecure default settings, limited vendor oversight, and insufficient training. Therefore, understanding user behaviour needs requires consideration not only of individual awareness and actions but also of the technical and organisational environment in which such behaviour occurs.

Furthermore, diversity of educational institutions also further complicated the design of awareness programmes. For instance, primary and secondary students differ in their level of independence and their ability to understand digital risk. Besides, vocational and university students may use different systems and encounter different forms of exposure. Teachers are responsible for handling student information while also modelling appropriate digital practices. Administrators make decisions about funding, technology procurement and the organisation of staff training. Research in vocational education and teacher professional development suggests that cybersecurity capability varies according to role and context, which limits the usefulness of uniform training approaches (Fadli et al., 2025; Leung et al., 2026).

Another problem concerns how awareness interventions are evaluated. Many studies report short-term improvements in knowledge, attitudes, awareness scores or self-reported intentions, but fewer examine whether these changes are maintained over time or lead to safer behaviour in practice. Interactive and gamified approaches, including school-based H5P activities, have produced measurable short-term improvements, although the available evidence does not yet show whether these gains are retained or transferred to real cybersecurity situations (Andria et al., 2025). Organisational approaches such as maturity frameworks and collaborative response models may also strengthen institutional preparedness, but their success depends on leadership support, available resources, technical capacity and local governance conditions (Almomani et al., 2021; Ootom et al., 2025). Longer-term evaluation is therefore needed to determine whether immediate learning outcomes develop into sustained behavioural and institutional improvement.

This review addresses that fragmentation by integrating behavioural, pedagogical and governance evidence. It asks three questions: (1) what threat and vulnerability patterns dominate recent educational cybersecurity research, (2) which awareness and training approaches show credible evidence of effectiveness, and (3) which institutional conditions enable or constrain sustained secure behaviour? This review contributes to cybersecurity awareness by integrating behavioral, pedagogical and governance evidence from a joint PMT and STS perspective, thus bridging individual threat appraisal and self-efficacy with the technical and organizational conditions that allow secure behavior. It also identifies the continuing gap between short-term improvements regarding cybersecurity knowledge and evidence of sustained secure behavior, highlighting the need for continuous and behaviour-oriented evaluation. Finally, the review shifts the lens of cybersecurity awareness from an individual responsibility to an institutional capacity, showing how the training effectiveness is shaped through secure system design, governance, role-specific support and organizational feedback. It also offers more cohesive basis for understanding how educational institutions might translate cybersecurity awareness into sustained protective practice.

Literature Review

Cybersecurity Awareness as a Behavioural and Organizational Construct.

Based on the literatures, PMT provides a useful basis for understanding how individuals respond to cybersecurity threats. Rogers (1975) explains protective behaviour through two related processes. Threat appraisal concerns how individuals judge the seriousness of a threat and their own vulnerability to it, while coping appraisal concerns whether they believe the recommended response will be effective and whether they are capable of carrying it out.

This distinction is relevant in educational settings because recognising a cybersecurity threat does not necessarily lead to secure behaviour. A student or staff member may understand the risks associated with phishing or data misuse but still fail to act appropriately when protective procedures are difficult to follow or when confidence in responding is low. Leung et al. (2026), for example, linked educators' data-protection practices with perceived vulnerability, risk perception and self-efficacy. Their findings suggest that awareness alone does not fully explain whether protective action takes place.

PMT focuses primarily on how individuals interpret threats and decide whether to adopt protective actions. This emphasis means that the theory says less about the institutional setting in which those decisions take place. STS theory helps address that gap by considering how social and technical elements operate together within an organisation. Bostrom and Heinen (1977) argue that organisational performance depends on how these subsystems interact. Applied to educational cybersecurity, this suggests that secure behaviour is influenced by more than individual motivation. Institutional policies, available technologies, access controls and administrative procedures also shape what users are able to do. A school, for example, may provide appropriate cybersecurity training but still face substantial risk if devices are poorly maintained or third-party applications are not adequately controlled.

Institutional conditions can also weaken otherwise strong technical measures. Security procedures that are difficult to follow or that disrupt normal teaching and administrative work may encourage users to find alternative ways of completing their tasks. These workarounds can introduce new vulnerabilities. STS is therefore useful for explaining why secure behaviour depends partly on whether institutional systems make the expected protective actions practical and workable.

Integrating PMT with STS provides a wider basis for assessing cybersecurity awareness by considering both individual responses and the surrounding technical and organisational context. Evaluation should therefore extend beyond of recall security advice immediately after training. It should also consider whether user can identify threats, report incidents, manage credentials safely and apply appropriate protective settings in practice. At the organisational level, attention should be given to whether incidents and recurring problems lead to changes in policy, training or technical controls. Viewed together, PMT and STS connect individual motivation with the institutional conditions that support or hinder secure behaviour.

Current Evidence and the Unresolved Gap

Three broad directions have been identified through sustainable recent studies. The first involves a shift from awareness messages towards examines school-wide and national

frameworks that address cybersecurity at broader organisational level. In this context, national strategy alignment, maturity assessment and collaborative incident response are treated as mechanisms for sustaining cybersecurity capability (AlDaajeh et al., 2022; Almomani et al., 2021; Ootom et al., 2025). Second, pedagogical research is moving toward multimedia, serious games and interactive environments. A systematic review of 119 multimedia tools found considerable design diversity but also uneven evaluation quality, while later school-based studies provide stronger evidence that interactive learning can improve short-term awareness (Zhang-Kennedy & Chiasson, 2021; Andria et al., 2025). Third, recent work pays greater attention to data ethics, local context and role-specific needs, including student data protection, vocational learners, teachers and culturally specific school frameworks (Amo-Filva et al., 2023; Chahid et al., 2026; Fadli et al., 2025; Leung et al., 2026).

The unresolved problem remains integration. For many behavioural studies the infrastructure and governance are not well specified. Technical or maturity frameworks may under-specify user perceptions of threats and confidence development. Pedagogical interventions tend to measure short-term gains in knowledge rather than long-term behaviour. Hence, the literature needs a model that links individual motivations with institutional affordances and feedback. The PMT-STS combination is used in this review to organize that connection and identify where the current evidence is strong, suggestive and where it is insufficient.

Methodology

This study used a structured critical literature review to examine evidence drawn from behavioural, educational and information-systems research. This approach was selected because the purpose of the review was to compare findings across different study designs, identify areas of disagreement and interpret their broader implications rather than calculate a pooled effect size. The search and selection process was conducted using explicit procedures for database searching, eligibility assessment and study selection, following established guidance for structured reviews (Grant & Booth, 2009; Snyder, 2019). Study identification and screening were also informed by PRISMA 2020. The process included duplicate removal, title and abstract screening, full-text assessment and final inclusion of eligible studies (Page et al., 2021).

The literatures reviewed covered Scopus, Web of Science, IEEE Xplore and ERIC academic research database. These databases were selected because together they provide coverage of information systems, computer science, educational technology and education research. Search terms were organised around three main areas: cybersecurity awareness and digital safety, educational settings, and relevant interventions or governance approaches. One Boolean combination used in the search was ('cybersecurity awareness' OR 'digital safety' OR 'cyber resilience') AND ('school' OR 'educational institution' OR 'higher education') AND ('training' OR 'curriculum' OR 'framework' OR 'governance'). Studies published between 2021 and 2026 were considered.

This period was chosen to reflect recent developments associated with the rapid expansion of digital learning and the increasing use of AI-enabled and platform-based educational technologies.

Eligibility criteria were defined before the final screening stage. The review included peer-reviewed journal articles and conference papers published in English between 2021 and 2026.

To be included, a study had to address cybersecurity awareness, behaviour, education, governance or related data-protection practices within primary, secondary, vocational or higher education. Studies dealing only with corporate environments were excluded, as were technically focused studies on cryptographic mechanisms that did not include an educational or human dimension. Backward and forward citation checking was used as an additional search strategy to locate relevant studies that may not have been captured through the database searches.

The PRISMA-informed study-selection process comprised identification, duplicate removal, title and abstract screening, full-text eligibility assessment and final inclusion. The database searches yielded 245 records. After 85 duplicates were removed, 160 titles and abstracts were screened against the predefined eligibility criteria. Forty-two articles proceeded to full-text assessment, of which 15 studies were retained as the core analytical corpus. The final synthesis prioritised studies that directly addressed the research questions and collectively represented behavioural, pedagogical, governance and technological dimensions.

The identification phase yielded 245 records. After removal of 85 duplicates, 160 titles and abstracts were screened. The relevance and methodological contribution of 42 full texts were assessed, and 15 studies were kept as the core analytical corpus. The selection process was deliberately restrictive in the synthesis stage. The review was limited to studies that directly addressed the research questions and collectively spanned behavioural, pedagogical, governance and technological dimensions. This does reduce the scope but increases analytical coherence.

Data were extracted into a structured matrix containing publication year, educational context, study design, intervention or framework, principal findings and relevance to PMT or STS constructs. The analysis followed thematic synthesis, moving from descriptive codes to higher-order categories (Thomas & Harden, 2008). Study quality was considered during interpretation rather than used as a rigid exclusion threshold because the corpus included surveys, design-science studies, systematic reviews, mixed-methods research and framework-development papers that cannot be ranked meaningfully with a single instrument.

The synthesis has two safeguards against over-claiming. First, findings from short-term or single-site interventions are treated as context-specific rather than universal. Second, the review distinguishes evidence of increased knowledge from evidence of sustained secure behaviour. This distinction is central because the field frequently measures the former while making claims about the latter.

Methodology: A Critical Literature Review of Cybersecurity Awareness in Education**CRITICAL LITERATURE REVIEW DESIGN**

DEFINED: Evaluates competing theories and synthesizes diverse perspectives to reveal hidden conceptual gaps.

**MULTI-DATABASE SEARCH (2021–2026)**

SOURCES: Queried Scopus, Web of Science, IEEE Xplore, and ERIC using specific Boolean strings.

INITIAL IDENTIFICATION 245 records
Iterative review of titles/abstracts, full-texts, and methodological quality to ensure eligibility.

FULL-TEXT ELIGIBILITY ASSESSMENT 42 articles

FINAL CORE SYNTHESIS 15 articles

**THREE-STAGE
SCREENING PROCESS
&
PRISMA-BASED
SELECTION RESULTS**

THEORETICAL FRAMEWORK

FOUNDATION: Objectives aligned with Protection Motivation Theory (PMT) and Socio-Technical Systems Theory.

**QUALITY APPRAISAL
& TRIANGULATION**

EVALUATION: Studies evaluated via CASP and MMAT tools with cross-checking by two researchers.

THEMATIC SYNTHESIS APPROACH

TRANSFORMATION: Data transformed through initial coding into descriptive themes and overarching analytical insights.

Figure 1: Review Design and Study Selection Process**Table 1: Characteristics Of The 15 Core Studies**

Study	Context	Primary Focus	Method/ Approach	Contribution to Synthesis
AlDaajeh et al. (2022)	National higher education	National strategy and curriculum alignment	Strategic plan and competency mapping	Shows that curriculum effectiveness depends on alignment with national capability goals.
Almomani et al. (2021)	Saudi higher education	Cybersecurity maturity assessment	Framework mapping and assessment-tool development	Operationalizes institutional maturity and gap analysis rather than awareness alone.
Amo-Filva et al. (2023)	Educational data protection	Student data ethics and prevention	Ethical and policy analysis	Frames data protection as a precautionary governance obligation.
Andria et al. (2025)	Elementary and junior secondary, Indonesia	Gamified awareness learning	R&D design with pre/post field testing	Finds short-term awareness gains after H5P-based interactive learning.
Arishi et al. (2024)	Primary and secondary schools	Awareness practices and barriers	Systematic review	Identifies serious games, mobile tools, curriculum inconsistency and resource constraints.
Barbu et al. (2023)	e-Learning students	Risk perception and threat understanding	Empirical analysis of student perceptions	Shows a gap between recognizing threats and knowing how to protect against them

Study	Context	Primary Focus	Method/ Approach	Contribution to Synthesis
Castillo & Anand (2025)	Schools	AI-supported cybersecurity awareness	Framework-oriented conference study	Connects AI-enabled learning with NIST-aligned awareness activities.
Chahid et al. (2026)	Secondary schools, Morocco	Social-media threats and awareness framework	Design science and quasi-experimental evaluation	Integrates learning, policy, technical safeguards and monitoring in a context-specific model.
Fadli et al. (2025)	Vocational high schools, Indonesia	Comparative awareness across disciplines	Objective knowledge assessment	Demonstrates meaningful differences in awareness across vocational programmes.
Jalil et al. (2024)	Secondary schools, Malaysia	Post-pandemic student awareness	Awareness assessment / programme evaluation	Supports targeted school-level awareness development after expanded digital learning.
Leung et al. (2026)	Teachers, Hong Kong	Data protection and media literacy	Quantitative survey of 120 teachers	Links protective strategies with awareness, perceived vulnerability and self-efficacy.
Lorenz (2025)	K-12 schools	School cybersecurity readiness	Mixed-methods school self-assessment	Treats cybersecurity as a school-wide maturity and culture issue.
Malasowe et al. (2024)	Educational technology environments	EdTech threats and controls	Review and case-based synthesis	Shows that user education must operate alongside risk assessment, access control and incident response.
Otoom et al. (2025)	Higher education / national collaboration	Collaborative incident response	Design science and stakeholder evaluation	Proposes EduCERT as a mechanism for shared awareness and coordinated response
Zhang-Kennedy & Chiasson (2021)	Non-expert learners / education tools	Multimedia cybersecurity education	Systematic review of 119 tools	Finds broad design innovation but uneven evidence and evaluation practices.

Generalization of the Main Statements

Threat Exposure Is Increasing Faster Than Risk Understanding

As digital education takes off, institutions are facing a wider range of cybersecurity risks across cloud services, personal devices, third-party applications and connected systems. Malasowe et al. (2024) identified threats such as phishing, ransomware, credential theft, insider risks, insecure IoT devices and third-party services with vulnerabilities. Barbu et al. (2023) also observed that students might know about common online dangers but may not be confident about how to respond to them. From a PMT perspective, awareness of a threat is unlikely to translate into consistent protective behaviour when users are uncertain about what to do or whether they can do it.

This shows that the problem is not just in the provision of information. Educational institutions are often deploying new digital platforms in contexts where ease of use, flexibility of teaching and security needs are not always convergent. Access policies, staff training or vendor oversight may not be fully updated before new tools are deployed. In these circumstances the cybersecurity risk is the interaction between user behavior and institutional conditions. For example, a phishing attempt may have more serious consequences where identity controls are weak, and poorly integrated systems may increase the likelihood of inappropriate data handling. Awareness programs therefore need to be aware of the systems and procedures in which users are expected to operate.

In addition, recent advances in artificial intelligence only complicate the picture. Generative AI could make social-engineering content more convincing and could also introduce additional data flows as educational content or user data are processed through AI-enabled platforms. Castillo and Anand (2025) note the importance of linking AI-powered cybersecurity education with recognized NIST functions. In addition to educational and policy measures, Chahid et al. (2026) include monitoring and technical safeguards. The findings from these studies show that awareness raising activities need to adapt to new threats but remain connected to institutional controls and clear reporting procedures.

Behavioural Vulnerability Is Primarily a Coping-Capability Problem

Across the corpus, differences in cybersecurity behaviour are better explained by capability and context than by a simple informed-versus-uninformed distinction. Fadli et al. (2025) found significant differences in awareness across vocational programmes, indicating that curriculum exposure and routine use of digital systems shape what students know. Leung et al. (2026) found that teacher data-protection strategies were associated with awareness, perceived vulnerability and self-efficacy. These findings support PMT, but they also imply that self-efficacy is partly produced by organizational conditions. Users are more likely to act when procedures are understandable, tools are usable and support is available.

Training design should reflect the different responsibilities users have within educational settings. Rather than focusing only on threat recognition, programmes need to prepare users for the actions they may be expected to take when a security problem occurs. Students, for example, may benefit from practising how to recognise suspicious requests and protect their credentials. Teachers require clearer routines for managing student information across email, cloud platforms and social media, while administrators need to understand issues such as

vendor risk, incident escalation and organisational responsibility. From this perspective, cybersecurity awareness is not simply a matter of knowing that threats exist. It also depends on whether users feel capable of responding and whether institutional systems support the actions expected from them.

The evidence also cautions against moralizing user error. The human-firewall metaphor can focus attention on the user at precisely the point where system design should be examined. If users repeatedly bypass controls, the relevant question is not only why they failed to comply but whether the control fits the task. STS theory directs the analysis toward this fit and makes clear that secure behaviour is co-produced by policy, technology and work design. Arch consistently shows that as digital education expands, it creates new vulnerabilities faster.

Interactive Learning Is Promising, but Long-Term Effectiveness Is Under-Evidenced

Pedagogical innovation is one of the strongest themes in the recent literature. Zhang-Kennedy and Chiasson (2021) identified a large and diverse set of multimedia awareness tools and argued for more systematic design and evaluation. Later evidence provides a more concrete basis for school use. Andria et al. (2025) reported improvements in awareness among elementary and junior secondary students after using an H5P-based game. Arishi et al. (2024) likewise found that serious games, mobile applications and tailored learning approaches are recurrent effective practices in the school literature.

However, the evidence does not justify the stronger claim that gamification produces durable secure behaviour. Most intervention studies measure knowledge, awareness scores or immediate performance over short periods. Few track whether learners resist real phishing attempts months later, maintain password hygiene or report incidents more consistently. This is a binding evidence constraint. The field has become better at making cybersecurity learning engaging, but it has not yet demonstrated that engagement reliably persists as behaviour.

A stronger evaluation design would combine knowledge measures with behavioural tasks, delayed follow-up and institutional outcomes. For example, a school could assess recognition of simulated phishing, reporting latency and recurrence of unsafe practices at multiple time points. Training should also be age-appropriate and role-specific. The core principle is continuity. A curriculum that revisits threats as technologies and learner responsibilities change may provide a more sustainable approach than a one-off annual seminar.

Governance Determines Whether Awareness Becomes Organizational Resilience

Governance affects whether cybersecurity awareness can be maintained beyond individual training activities. Almomani et al. (2021) addressed this issue through a maturity assessment framework for higher education institutions. The framework helps institutions locate weaknesses and decide where improvement is needed. Otoom et al. (2025) considered governance at an inter-institutional level through EduCERT, where coordinated incident response and knowledge sharing form part of a collaborative approach. AlDaajeh et al. (2022) examined the issue from a national perspective and linked cybersecurity education with broader capability development and workforce needs. These studies approach governance at different levels, but each places institutional arrangements alongside individual awareness.

Student data protection presents a related concern. Amo-Filva et al. (2023) uses the precautionary principle to argue that compliance requirements alone may not address all of the consequences associated with unauthorized disclosure. This is particularly relevant in education because decisions about digital platforms also involve decisions about how student information is handled. Whether a platform performs its intended function is therefore not the only concern. Institutions must also examine what information is collected, how access is managed and what responsibility vendors carry when student data are involved.

Lorenz (2025) examines the same institutional issue at the school level by treating cybersecurity readiness as something shaped by school policies and existing safeguards, together with staff capability. This view makes follow-up particularly important. Problems identified during training may reveal difficulties that cannot be solved simply by providing users with more information. Incident reports can similarly indicate weaknesses in procedures or technical controls. Schools can use these findings when reviewing their policies, technologies or training practices. Without that follow-up, awareness activities may have little connection with the way cybersecurity problems are actually identified and addressed within the institution.

PMT-STS Interpretation of Cybersecurity Awareness

The synthesis supports a four-stage interpretation. First, the institution establishes technical and governance conditions through identity management, secure platforms, vendor controls, data policies and leadership priorities. Second, users encounter threats and form threat appraisals about severity and vulnerability. Third, coping appraisal depends on response efficacy and self-efficacy, both of which are shaped by training quality, task design and access to support. Fourth, behaviour and incidents feed back into institutional learning. Security culture emerges from repeated adjustment across these stages rather than from awareness messaging alone.

This model explains why identical training can produce different outcomes across institutions. A high-resource university with mature identity management and a functioning incident-response process gives users clearer protective options than a school with fragmented systems and minimal support. The same applies within institutions. Teachers who routinely handle sensitive student records require different controls and learning tasks from younger students using classroom applications. PMT describes the user's decision process. STS explains why the decision process is enabled or constrained.

The model also identifies a leverage point for management: reduce the gap between expected secure behaviour and the effort required to perform it. Training can increase self-efficacy, but usability, clear escalation routes and secure defaults can reduce the behavioural burden more directly. This suggests that the most effective awareness strategy is partly an information-systems design strategy.

Discussion

This review indicates that educational cybersecurity awareness should be reframed from a communication problem to a capability-management problem. The dominant weakness in the literature is not a lack of recommendations. Studies repeatedly call for training, stronger policy, technical controls and collaboration. The weaker point is causal evidence showing which

combinations produce durable outcomes under real institutional conditions. As a result, a journal contribution in information systems and technology management should resist simple prescriptions and instead specify the organizational mechanisms through which awareness is expected to work.

PMT clarifies one mechanism. Threat information matters when users believe they are vulnerable and that the consequences are material, but fear-oriented messaging can fail if users do not know what to do or doubt that the response will work. This highlights the need of effective coping-oriented content programmes that can strengthen users' ability and confidence to respond appropriately. Therefore, simulated decision tasks, guided configuration of privacy settings, phishing reporting exercises, and role-specific scenarios may provide more practical learning experiences than generic lectures by translating the protective response into concrete and actionable practices. Leung et al. (2026) provides direct support for the importance of self-efficacy among teachers, while school-based gamification studies demonstrate how interactive formats can build confidence and engagement among users (Andria et al., 2025).

STS adds an institutional dimension to the analysis. Cybersecurity awareness is unlikely to compensate for weak system design or inadequate governance when users operate within poorly supported environments. Studies on maturity assessment, EdTech risk management and collaborative incident response indicate that institutions need established procedures for identifying vulnerabilities, assigning responsibility and learning from incidents (Almomani et al., 2021; Malasowe et al., 2024; Otoom et al., 2025). Management therefore has a direct role in shaping secure practice. This includes allocating adequate resources, reviewing vendor-related risks and giving staff sufficient time and support for training. When unsafe workarounds occur repeatedly, the problem may also lie in the system or procedure rather than solely in user behaviour.

Educational responses also need to reflect differences between user groups. In primary and secondary settings, cybersecurity learning needs to match learners' age and level of digital independence. Vocational students may require scenarios connected to the systems and risks encountered within particular occupational areas (Fadli et al., 2025). For teachers, professional development needs to extend beyond general awareness by addressing media literacy, data protection and practical routines for handling digital information (Leung et al., 2026). Higher education presents a different challenge because cybersecurity responsibilities are often distributed across faculties, administrative units and central IT services. A uniform awareness programme is therefore unlikely to address the range of risks and responsibilities found across these settings.

Several implications for policy emerge from this evidence. Cybersecurity education needs to be repeated over time and adapted to the roles of different users. Practical exercises are also important because knowing about a threat does not necessarily mean that a user can respond appropriately when it occurs. Awareness activities should therefore be connected with data governance, platform design and institutional procedures. Evaluation also needs to extend beyond immediate post-training questionnaires. Recent school frameworks and national cybersecurity education strategies point in this direction (AlDaajeh et al., 2022; Chahid et al., 2026; Lorenz, 2025).

The evidence base, however, remains uneven. Many studies report short-term improvements in knowledge, awareness or confidence, while fewer examine whether these changes persist or influence behaviour over longer periods. This imbalance may produce an overly positive picture of awareness interventions, although the available studies do not allow the extent of such bias to be determined. Future research would benefit from longitudinal designs and clearer definitions of outcomes. Where appropriate, preregistered evaluation could also reduce analytical flexibility. Assessment should move beyond knowledge scores to include observed protective behaviour, confidence in responding to threats and institutional indicators such as incident-reporting time or remediation progress. Replication across countries and educational settings is also needed because available resources, regulatory conditions and technology access differ considerably between contexts.

Generative AI introduces another layer to these existing concerns. Its relevance lies partly in the ease with which convincing social-engineering content can now be produced and partly in the new data flows created when educational material or student information is submitted to AI systems. These developments can be examined within the same PMT-STs framework rather than treated as a separate cybersecurity problem. Future studies could test whether training that includes AI-related threat scenarios improves users' ability to identify realistic attacks. Research should also examine how institutions can establish appropriate data-use controls without creating procedures that are so restrictive or cumbersome that users routinely bypass them.

The present review has limitations. It is restricted to English-language peer-reviewed sources and a recent publication window. Its critical-review design prioritizes conceptual integration over exhaustive coverage, and the 15-study core corpus is heterogeneous in context and method. These characteristics preclude meta-analysis and limit claims about comparative effect size. The review also relies heavily on self-reported or short-term outcomes because that is what the current literature provides. These limitations strengthen, rather than weaken, the argument for better longitudinal and behavioural evaluation.

The synthesis of only 15 final core studies also met the predefined inclusion and quality criteria through a multi-stage screening process designed for conceptual integration and analytical rigor namely; 1) Initial Database Search & Screening whereby a systematic query across four databases (Scopus, Web of Science, IEEE Xplore, and ERIC) yielded 245 initial records. After removing 85 duplicates, 160 titles and abstracts were screened for initial relevance, 2) Full-Text Inclusion Assessment: From the remaining records, 42 full-text articles were evaluated against predefined eligibility criteria, specifically requiring peer-reviewed studies published between 2021 and 2026 that directly addressed cybersecurity awareness, behavior, governance, or data protection in educational settings, and Final Synthesis Rationale: During the final selection stage, the paper narrowed the synthesis corpus to 15 core studies that met quality and analytical standards. Rather than maximizing total quantity, this targeted sample was chosen because it directly answered the core research questions and collectively represented key behavioral (PMT), pedagogical, governance (STs), and technological dimensions necessary for a coherent synthesis.

Conclusion

Cybersecurity awareness in educational institutions should be viewed as part of a wider socio-technical system rather than as an issue of individual behaviour alone. The reviewed studies show that users' responses to cyber threats are influenced by their knowledge and confidence, but also by the systems, policies and support available within the institution. This makes it difficult to treat awareness campaigns as a sufficient response to cybersecurity risk. Where institutional controls are weak or difficult to use, improvements in user awareness may not translate into safer practice.

The evidence on interactive and gamified learning is generally positive in the short term, especially for younger learners. However, most studies measure immediate changes in knowledge or awareness, so it remains unclear whether these effects are maintained over time or lead to sustained behavioural change. For this reason, cybersecurity education is likely to be more useful when it is delivered continuously and adapted to the responsibilities of different user groups. Training also needs to operate alongside secure system design, institutional assessment and effective incident-response procedures.

For schools and higher education institutions, this means that cybersecurity awareness should form part of routine institutional practice rather than depend on occasional training sessions. Students, teachers, administrators and technical staff face different risks and responsibilities, so a single training approach is unlikely to address all of their needs. Institutions should also evaluate whether awareness activities lead to changes in actual behaviour and whether users can report and respond to incidents effectively. Recurring unsafe practices should therefore prompt attention to training, but they should also lead institutions to examine whether existing systems, procedures or governance arrangements are contributing to the problem.

Acknowledgements:	The authors would like to express their sincere appreciation to UiTM Kedah for providing the necessary support for this research project
Funding Statement:	No Funding
Conflict of Interest Statement:	The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the Journal of Information System and Technology Management (JISTM)
Ethics Statement:	This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards
Author Contribution Statement:	All authors contributed significantly to the development of this manuscript. Siti Rafidah Muhamat Dawam and Nor Hafizah Abdul Razak contributed to the conceptualization, methodology of the study and manuscript drafting. Mazura Mat Din and Shaifizat Mansor contributed to literature search and synthesis. Nurul Husna Mahadzir contributed to language refinement, critical revision, and final approval of the manuscript.
Pengisytiharan Penggunaan Kecerdasan Buatan (AI)	“The author(s) declare that generative AI or AI-assisted technologies were used during the preparation of this manuscript. The following tool(s) were used: ChatGPT. The tool was used for language editing and grammar improvement. All AI-assisted content was reviewed and verified by the author(s), who take full responsibility for the accuracy, originality, integrity, and final content of the manuscript.”

References

- AlDaajeh, S., Saleous, H., Alrabae, S., Barka, E., Breiting, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119, 102754. <https://doi.org/10.1016/j.cose.2022.102754>
- Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science*, 7, e703. <https://doi.org/10.7717/peerj-cs.703>
- Amo-Filva, D., Garcia-Holgado, A., Fonseca, D., Garcia-Holgado, L., & Garcia-Penalvo, F. J. (2023). Precautionary principle for students' data protection. In *Proceedings of the 13th International Conference on Virtual Campus (JICV 2023)*. IEEE. <https://doi.org/10.1109/JICV59748.2023.10565717>
- Andria, A., Laksono, R. D., Sussolaikah, K., Mat Din, M. B., Mansor, S., & Dawam, S. R. M. (2025). Assessment of cyber security awareness using developed game from H5P on users aged at elementary and first secondary school in Madiun City. *Journal of Applied Engineering and Technological Science*, 7(1), 539-549. <https://doi.org/10.37385/jaets.v7i1.6705>
- Arishi, A. A., Kamarudin, N. H., Abu Bakar, K. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity awareness in schools: A systematic review of practices, challenges, and target audiences. *International Journal of Advanced Computer Science and Applications*, 15(12). <https://doi.org/10.14569/IJACSA.2024.0151249>
- Barbu, M., Zamfiroiu, A., Marinescu, I. A., Iordache, D., & Bumbac, R. (2023). Empowering digital education: Understanding students' perceptions about risks and threats in the shifting educational paradigm. *Studies in Informatics and Control*, 32(4), 105-114. <https://doi.org/10.24846/v32i4y202310>
- Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS Quarterly*, 1(3), 17-32. <https://doi.org/10.2307/248710>
- Castillo, G., & Anand, S. (2025). Using AI to boost cybersecurity awareness: Implementing the NIST framework in schools. In *Technology and Innovation in Learning, Teaching and Education (Communications in Computer and Information Science, Vol. 2481, pp. 112-127)*. Springer. https://doi.org/10.1007/978-3-032-02669-9_10
- Chahid, A., El Marzak, Y., & Mansouri, K. (2026). Developing a cybersecurity awareness framework to safeguard Moroccan students from social media threats. *Frontiers in Education*, 11, 1719173. <https://doi.org/10.3389/feduc.2026.1719173>
- Fadli, R., Eliza, F., Sari, R. C., Surjono, H. D., Khulanthaivel, G., & Kartika, R. (2025). Comparison of cybersecurity awareness among vocational high school students. *International Journal on Advanced Science, Engineering and Information Technology*, 15(6), 1747-1754. <https://doi.org/10.18517/ijaseit.15.6.20304>
- Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), 91-108. <https://doi.org/10.1111/j.1471-1842.2009.00848.x>
- Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaiah, M. A. (2024). Cybersecurity awareness among secondary school students post Covid19 pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 37(1), 115-127. <https://doi.org/10.37934/araset.37.1.115127>

- Leung, S. L. T., Ho, W., & Tam, W. K. C. (2026). Professional development in enhancing teachers' cybersecurity awareness: Current status and future directions of media literacy training. *Education Sciences*, 16(2), 196. <https://doi.org/10.3390/educsci16020196>
- Lorenz, B. (2025). Improving cybersecurity education in schools: An assessment of the 'Digitally Safer School' proposal. In *Learning and Collaboration Technologies: 12th International Conference, LCT 2025, Proceedings, Part I (Lecture Notes in Computer Science, Vol. 15806, pp. 315-327)*. Springer. https://doi.org/10.1007/978-3-031-93564-0_19
- Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and best practices for handling cybersecurity risks in educational technology environment (EdTech). *NIPES Journal of Science and Technology Research*, 6(2), 293-311. <https://doi.org/10.5281/zenodo.12617068>
- Otoom, A. A., Atoum, I., Al-Harashseh, H., Aljawarneh, M., Al Refai, M. N., & Baklizi, M. (2025). A collaborative cybersecurity framework for higher education. *Information & Computer Security*, 33(3), 362-389. <https://doi.org/10.1108/ICS-02-2024-0048>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114. <https://doi.org/10.1080/00223980.1975.9915803>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333-339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, 8, 45. <https://doi.org/10.1186/1471-2288-8-45>
- Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys*, 54(1), Article 12. <https://doi.org/10.1145/3427>