Cybersecurity Leadership as Governance: A Constructivist Grounded Theory of Digital Risk Stewardship in Public Education

Zul Afida Abdullah., Roshafiza Hassan

Faculty of Educational Studies Universiti Putra Malaysia

DOI: https://doi.org/10.47772/IJRISS.2026.10200330

Received: 21 February 2026; Accepted: 26 February 2026; Published: 09 March 2026

ABSTRACT

Digital transformation has intensified reliance on digital infrastructures within public education while simultaneously amplifying institutional exposure to cybersecurity risks. Yet educational leadership scholarship continues to privilege innovation and digital maturity, leaving cybersecurity under-theorised as a governance responsibility. Addressing this gap, this study developed a constructivist grounded theory of Cybersecurity Leadership within Malaysia's public education system. Drawing on 26 semi-structured interviews across school, district, and policy levels, constant comparative analysis generated a multidimensional governance model. Findings reveal a governance internalisation process in which digital risk shifts from delegated technical management to executive accountability. Six interdependent dimensions were identified: strategic governance integration, risk-informed decision-making, cultural reinforcement, capability development, crisis leadership, and ethical stewardship. Through their recursive interaction, these dimensions generate institutional resilience and digital trust. The study reframes cybersecurity as a core executive leadership competency embedded within strategic direction-setting rather than a peripheral compliance function. By integrating socio-technical systems and organisational resilience perspectives, it advances digital leadership theory beyond innovation-centric paradigms and positions risk-informed governance as a foundational principle of sustainable digital transformation in public education.

Keywords: cybersecurity leadership, digital governance, educational leadership, grounded theory, organisational resilience, Malaysia

INTRODUCTION

Digital leadership scholarship has predominantly equated digital progress with technological adoption, innovation capability, and transformation readiness (Perifanis & Kitsios, 2023; Garcez et al., 2022; Aras & Büyüközkan, 2023). Within educational contexts, leaders are frequently positioned as catalysts of innovation who cultivate technology-enabled pedagogical reform (Assefa & Mujtaba, 2025). While such framing has advanced important insights into digitally mediated change, it has also produced a conceptual asymmetry: digital expansion is extensively theorised, whereas digital vulnerability remains marginal within leadership discourse. In privileging innovation and digital maturity, prevailing frameworks risk treating cybersecurity as an operational afterthought rather than as a constitutive dimension of governance.

This imbalance is not merely theoretical; it carries structural implications. When cybersecurity is framed primarily as a technical safeguard or compliance mechanism (Atasever & Özen, 2025), responsibility is often delegated to ICT units, thereby insulating executive leadership from direct accountability for digital risk. Such delegation implicitly constructs a separation between transformation and protection, as though institutional growth and institutional security operate in parallel rather than interdependent trajectories. Corporate governance research has increasingly challenged this separation by positioning cybersecurity as a board-level strategic responsibility (Alsulami, 2026). However, educational leadership theory has yet to fully internalise this shift. As a result, digital leadership models in education may inadvertently normalise a governance architecture in which innovation is centralised while risk stewardship remains peripheral.

Furthermore, interdisciplinary research underscores that cybersecurity effectiveness is shaped not only by technical controls but also by socio-organisational vulnerabilities, including leadership culture, decision-making hierarchies, and behavioural norms (Khadka & Ullah, 2025). If leadership theory fails to account for these socio-technical interdependencies, it risks reproducing a technologically deterministic view of digital reform. Existing governance models derived largely from corporate contexts (Savaş & Karataş, 2022) offer limited guidance for public education systems characterised by bureaucratic layering, regulatory mandates, and distributed authority. Consequently, there remains a critical theoretical gap: educational leadership scholarship lacks a process-oriented explanation of how cybersecurity is enacted as governance within public institutions.

Taken together, these limitations suggest that digital leadership theory remains structurally under-integrated with risk governance. A framework that celebrates transformation without systematically integrating risk governance risks legitimising institutional fragility under conditions of digital intensification. If educational organisations are to sustain public trust in data-driven environments, cybersecurity cannot remain a peripheral compliance function; it must be theorised as an executive governance competency embedded within institutional direction-setting and accountability structures.

LITERATURE REVIEW

Digital Leadership and Innovation-Centric Paradigms

Digital leadership scholarship has consistently framed digital progress in terms of technological adoption, innovation capacity, and transformation readiness (Perifanis & Kitsios, 2023; Garcez et al., 2022; Aras & Büyüközkan, 2023). Within educational contexts, leaders are commonly positioned as drivers of technology-enhanced pedagogy and digital ecosystem development (Assefa & Mujtaba, 2025; Nguyen & Tuamsuk, 2022). These perspectives have significantly advanced understanding of digitally mediated organisational change.

However, this dominant framing produces conceptual asymmetry. While digital expansion and innovation are extensively theorised, digital vulnerability remains comparatively marginal within leadership discourse. Security is frequently treated as a technical safeguard or compliance requirement rather than as an executive governance responsibility (Atasever & Özen, 2025). As a result, digital leadership models risk privileging transformation while under-theorising risk stewardship.

Cybersecurity as Strategic Governance

Beyond educational contexts, governance scholarship increasingly positions cybersecurity as a strategic, board-level responsibility embedded within enterprise risk management and fiduciary oversight (Alsulami, 2026; García-Nieto et al., 2024; Qureshi & Koo, 2026). Frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (Pham & Nguyen, 2023) and ISO standards (Wissemann et al., 2022) reinforce expectations that leadership bodies must exercise structured oversight of cyber risk, incident response, and resilience planning.

This shift reframes cybersecurity from operational control to governance architecture. Cyber threats are recognised as enterprise-wide risks capable of undermining organisational continuity, reputation, and stakeholder trust. Accordingly, executive leaders are increasingly expected to define risk appetite, oversee compliance integration, and align cybersecurity with strategic direction.

Yet this governance reframing has not been fully translated into educational leadership theory. School and system leaders manage sensitive student data, cloud platforms, and networked infrastructures, but cybersecurity is often delegated to technical units without being conceptualised as part of leadership identity or governance capability (Watini et al., 2024).

Socio-Technical Systems and Organisational Resilience

Interdisciplinary research further demonstrates that cybersecurity effectiveness depends not only on technical infrastructure but also on socio-organisational dynamics. Human behaviour, cultural norms, decision-making

hierarchies, and accountability structures significantly shape institutional vulnerability (Khadka & Ullah, 2025; Wendt-Lucas et al., 2025). Socio-technical systems theory underscores that digital risk emerges from the interaction between technological systems and organisational structures rather than from technical weaknesses alone (Hanafizadeh & Mehrasa, 2025).

Complementing this perspective, organisational resilience scholarship emphasises adaptive capacity, coordinated crisis response, and institutional learning as key determinants of sustained performance under disruption (Dahmen, 2023; Pradana & Ekowati, 2024). From this lens, cybersecurity leadership extends beyond preventive controls to include preparedness, cross-level coordination, and post-incident reflection.

Despite these theoretical insights, there remains no empirically grounded model explaining how cybersecurity is enacted as governance within public educational systems, particularly in bureaucratically structured contexts such as Malaysia. Existing cybersecurity governance models are largely derived from corporate or private-sector environments (Savaş & Karataş, 2022), limiting their contextual applicability. This theoretical and contextual gap underscores the need to reconceptualise cybersecurity leadership as a socio-technical and resilience-oriented governance construct embedded within public educational administration.

Limitations

First, the study relied primarily on interview narratives within a single national context, which may limit transferability across decentralised systems. Second, documentary sources were used for contextual framing rather than full triangulated analysis. Third, as a constructivist grounded theory, the model prioritises processual explanation over statistical generalisability. Future multi-country comparative or mixed-method designs may strengthen empirical robustness.

METHODOLOGY

Research Design

This study adopted a constructivist grounded theory approach to generate a substantive theory of cybersecurity leadership within public educational systems. Constructivist grounded theory, as articulated by Hammar Chiriac et al. (2023), recognises that theory is co-constructed through the interaction between researcher and participants, making it particularly appropriate for exploring complex leadership practices embedded within socio-organisational contexts. Unlike positivist approaches that seek hypothesis testing, grounded theory facilitates the inductive development of conceptual categories directly from empirical data (Bobbink et al., 2024). Given the limited theorisation of cybersecurity leadership in educational governance, this methodological approach enabled the systematic generation of concepts grounded in participants lived experiences, policy environments, and institutional realities. Through iterative coding and constant comparison, the study moved beyond description to develop a process-oriented explanatory framework.

Grounded theory was selected due to its suitability in under-theorised domains and its capacity to develop context-sensitive explanatory models (Musole, 2026). In emerging areas such as cybersecurity leadership where established theoretical models are largely derived from corporate settings an inductive design allows for the discovery of locally embedded meanings, practices, and governance dynamics. Constructivist grounded theory further accommodates complexity, acknowledging multiple realities and the influence of cultural, structural, and institutional conditions on leadership behaviour (Kouam, 2025). For the Malaysian public education context, this approach was especially valuable in uncovering how leaders interpret cyber risk, negotiate bureaucratic constraints, and enact governance responsibilities within resource-limited environments. By privileging process over prescription, the methodology supports the development of a substantive theory that is empirically anchored, contextually relevant, and capable of informing both scholarship and policy.

The research design followed the core grounded theory procedures of theoretical sampling, constant comparative analysis, memo writing, and iterative category development, culminating in the constructing of a substantive theoretical model. Although the primary data source comprised semi-structured interviews, the analytic process was sensitised by reference to publicly available cybersecurity governance documents, national policy

statements, and international cybersecurity frameworks. These documents were not treated as primary empirical data but were used to contextualise leadership narratives and strengthen theoretical sensitivity. This approach aligns with qualitative governance research that recognises policy frameworks as interpretive backdrops rather than triangulated datasets (Paigude et al., 2024; Mishra et al., 2022).

Participants

Twenty-six participants were purposively selected to ensure rich, information-dense data capable of illuminating the processes underpinning cybersecurity leadership within public education. Purposive sampling is widely recommended in qualitative inquiry where the objective is depth of understanding rather than statistical generalisation (Safari et al., 2023). In grounded theory research specifically, participant selection is guided by theoretical relevance, enabling the researcher to engage individuals who possess direct experience with the phenomenon under investigation (Lian et al., 2025). The sample comprised educational leaders (e.g., school principals and senior administrators), ICT coordinators, cybersecurity officers, and policy stakeholders, thereby capturing diverse functional perspectives on governance, risk management, and digital implementation. This diversity strengthened analytic depth by enabling comparison across roles, responsibilities, and decision-making authority structures within cybersecurity practices.

Participants represented multiple levels of Malaysia's public education system, including school-level leadership, district or state administration, and central policy or regulatory units. Such multi-level representation aligns with recommendations in governance and organisational research that complex leadership phenomena should be examined across hierarchical layers to capture systemic interactions (Bento et al., 2023; Jalonen, 2025). This multi-level sampling strategy enabled cross-comparison of governance enactment across hierarchical layers and ensured analytic sensitivity to distributed leadership processes. In the context of cybersecurity, leadership enactment is distributed across strategic, operational, and technical domains, necessitating insights from actors positioned at different governance tiers. By incorporating perspectives from both policy architects and frontline implementers, the study identified patterns of coordination, accountability, and adaptive response across institutional levels. This design enhances the contextual sensitivity of the emerging theory and ensured that the resulting framework reflects the structural realities of Malaysia's public education ecosystem rather than a single organisational vantage point. Interviews continued until theoretical saturation was reached. Saturation was determined when additional interviews no longer produced new conceptual properties or dimensions within core categories, and when relationships between categories were sufficiently elaborated.

Data Collection

Semi-structured interviews were conducted to explore leadership practices, governance mechanisms, and institutional responses to cybersecurity risks across multiple levels of the public education system. Semi-structure interviews are particularly appropriate for examining complex organisational phenomena because they balance focused inquiry with flexibility, allowing participants to elaborate on experiences, interpretations, and contextual constraints (Reissner & Whittle, 2022). Guided by an interview protocol aligned with the study's emerging analytical categories, questions probed areas such as strategic oversight, policy implementation, incident management, inter-departmental coordination, and capacity-building initiatives. At the same time, the open-ended structure enabled participants to surface unanticipated issues, including informal practices, cultural barriers, and tacit leadership behaviours that may not be captured through structured instruments. This approach supported in-depth exploration of how cybersecurity governance is enacted in practice rather than merely described in policy documents.

Within a constructivist grounded theory framework, semi-structured interviews facilitate the co-construction of meaning between researcher and participant, enabling the development of analytically rich and process-oriented data (Urquhart et al., 2025). The interactive nature of the interviews allowed for probing, clarification, and theoretical sampling as concepts began to emerge, consistent with the constant comparative method originally articulated by Blown and Bryce (2022). Interviews also provide insight into how leaders interpret cyber risks, negotiate institutional constraints, and respond to emerging threats within bureaucratic and resource-limited environments. By foregrounding participants' narratives while maintaining analytic rigor, the use of semi-

structured interviews strengthened the study's capacity to generate a contextually grounded and empirically robust theory of cybersecurity leadership in public education.

Documentary Contextualisation of Cybersecurity Governance Environment

The governance categories presented in Table 1 conceptually align with, yet are analytically extended by, the six-dimensional model developed in this study. Specifically, the NIST CSF's emphasis on Organizational Context and Risk Management Strategy corresponds to the dimension of *Strategic Governance Integration*, where cybersecurity becomes embedded within institutional direction-setting rather than remaining a technical adjunct. Similarly, the categories of Roles, Responsibilities, and Authorities and Policy parallel the dimension of *Risk-Informed Decision-Making*, as both require explicit executive articulation of accountability, risk appetite, and structured governance procedures.

Table 1. Functions and categories of NIST CSF

Function	Category	Description
Govern	Organizational Context	Organization's mission, goal, stakeholder expectations, legal requirements.
	Risk Management Strategy	Priorities, constraints, risk appetite and tolerance statements, and assumptions of the organization are established, disseminated, and utilized to support operational risk decisions.
	Roles, Responsibilities, and Authorities	Establishment and communication of cybersecurity roles, responsibilities, and authorities to promote accountability.
	Policy	Cybersecurity policy is established, communicated, and enforced.
	Oversight	The outcomes and performance of risk management activities are utilized to inform, enhance, and modify the risk management strategy.
	Cybersecurity Supply Chain Risk Management	Supply chain risk management processes are identified, established, managed, monitored, and improved.

Source: Hossain (2024)

The Oversight category aligns closely with *Crisis Leadership* and *Ethical Stewardship*, as both emphasise continuous monitoring, evaluative feedback, and executive responsibility for safeguarding institutional integrity. Furthermore, Cybersecurity Supply Chain Risk Management resonates with the dimension of *Capability Development*, particularly in its recognition that resilience extends beyond internal controls to external dependencies and inter-organisational networks.

However, while NIST CSF provides a structured governance taxonomy, it primarily specifies what organisations should implement. The six-dimensional model developed in this study extends this structure by explaining how cybersecurity governance becomes internalised within leadership identity and organisational culture. In other words, Table 1 articulates governance architecture, whereas the grounded model explicates the process through which architecture becomes enacted, reinforced, and sustained within public education systems. While the primary focus of this study was inductive theory generation, established governance frameworks were used as interpretive reference points to situate the emerging model within broader cybersecurity governance discourse.

Data Analysis

Data were analysed using the constant comparative method, a central analytic procedure in grounded theory that involves systematically comparing incidents, codes, and emerging categories to develop conceptual depth and theoretical integration (Shava et al., 2025). The analysis began with open coding, during which interview transcripts were examined line-by-line to identify preliminary concepts related to cybersecurity leadership practices, governance mechanisms, and institutional responses to cyber risks. This stage prioritised analytic openness, allowing codes to remain closely grounded in participants' accounts while enabling patterns and variations to emerge inductively (Davidson et al., 2023). Through ongoing comparison within and across

interviews, initial codes were clustered into more focused categories that captured recurring processes and leadership enactments.

Subsequently, axial coding was conducted to explore relationships among categories by examining conditions, actions/interactions, and consequences associated with cybersecurity leadership enactment (Akkaya, 2023). During this phase, analytic attention focused on identifying how strategic oversight, risk deliberation, cultural reinforcement, and crisis coordination were interconnected within governance structures. Constant comparison enabled refinement of category properties and clarification of the structural and contextual factors shaping leadership responses. This stage facilitated the development of an integrated explanatory structure linking governance processes with institutional dynamics and environmental pressures.

Finally, selective coding was undertaken to refine and synthesise categories around a central core construct, culminating in the development of a substantive theoretical model (Christodoulou et al., 2025). The core category Cybersecurity Leadership as Governance Integration was identified through iterative comparison and memo analysis as the organising construct that linked all other dimensions. Theoretical saturation was reached when additional data no longer generated new conceptual properties or dimensions within the emerging framework and when relationships between categories were sufficiently elaborated and theoretically coherent (Daher, 2023; Bouncken et al., 2025).

Throughout the analytic process, memo writing accompanied coding to capture emerging insights, conceptual linkages, and theoretical propositions. These memos supported abstraction from descriptive accounts toward higher-level conceptualisation, ensuring that the resulting model remained empirically grounded while achieving theoretical integration.

Trustworthiness

Credibility was strengthened through member checking and peer debriefing, both of which are widely recognised strategies for enhancing trustworthiness in qualitative research (Kakar et al., 2023). Member checking involved sharing emerging interpretations and thematic summaries with selected participants to verify accuracy, resonance, and interpretive alignment with their experiences. This process helped minimise researcher bias and ensured that the developing theoretical categories authentically reflected participants' perspectives (Hossan et al., 2025). In addition, peer debriefing was conducted with experienced qualitative researchers who critically examined analytic decisions, challenged underlying assumptions, and refined conceptual interpretations. Such reflexive dialogue enhanced analytic rigour by exposing potential blind spots and strengthening the credibility of the emerging framework (Soysal & Türkmen, 2024).

Dependability was ensured through the systematic maintenance of audit trails and analytic memos. An audit trail documented methodological decisions, coding procedures, category development, and processes of theoretical integration, thereby providing transparency and enabling external review of the research process (Lim, 2025). Analytic memos served as reflexive records of emerging insights, conceptual linkages, and evolving theoretical propositions, supporting coherence and analytic depth throughout the grounded theory analysis (Khan & Khan, 2024; Paapa & Kambona, 2025). Transferability was supported through rich, thick description of participants, institutional settings, and governance structures, allowing readers to assess the applicability of the findings to other educational systems or policy environments (Kin Heng & Ng, 2025). Collectively, these strategies enhanced the overall trustworthiness and methodological robustness of the study.

Emergent Theoretical Model

The resulting model positioned Cybersecurity Leadership as a central governance construct rather than a peripheral technical function. The analysis demonstrated that cybersecurity was enacted as an executive leadership responsibility embedded within strategic oversight, institutional direction-setting, and accountability structures. Consistent with contemporary governance scholarship recognising cybersecurity as an enterprise-wide obligation requiring executive engagement (Efe, 2025), the findings revealed that educational leaders assumed stewardship over digital risk as part of core governance practice rather than delegated compliance.

Drawing on socio-technical systems theory, which foregrounds the interdependence of technological infrastructures and human agency (Hanafizadeh & Mehrasa, 2025), the model situated cybersecurity leadership within the broader governance architecture of public educational institutions. The grounded analysis identified six interdependent leadership dimensions that functioned as mutually reinforcing mechanisms. These dimensions collectively generated two systemic outcomes: Institutional Resilience and Digital Trust. In alignment with organisational resilience theory, resilience emerged not merely as resistance to disruption but as adaptive capacity, coordinated crisis response, and institutional learning (Mehta et al., 2024). Simultaneously, digital trust was constructed through sustained reliability, ethical data stewardship, transparency, and accountability in digitally mediated environments (Kesar, 2025).

Rather than treating cybersecurity as a technical safeguard, the model theorised it as a governance architecture through which leaders integrated strategic oversight, risk rationality, cultural stewardship, and ethical accountability. In this formulation, cybersecurity leadership operated as a structural condition of sustainable digital transformation simultaneously safeguarding institutional continuity and reinforcing stakeholder confidence.

Within this framework, cybersecurity leadership is conceptualised as: (1) a strategic governance function, ensuring alignment between cyber risk oversight and institutional mission (Mızrak, 2023); (2) a risk management mechanism, integrating threat identification, mitigation, and compliance within enterprise risk structures (Zamil et al., 2022); (3) a cultural transformation process, shaping security-aware norms and behaviours across the organisation (Quainoo, & Ahad, 2026); (4) a capacity-building strategy, enhancing digital competencies and preparedness among leaders and staff (Leung et al., 2026); (5) a crisis leadership competency, enabling decisive response and adaptive coordination during cyber incidents (Chavarnakul et al., 2025); and (6) an ethical stewardship responsibility, safeguarding data integrity, privacy, and public accountability (Nasir et al., 2025). The reinforcing interaction among these dimensions forms a cyclical and mutually constitutive system: governance informs culture, culture strengthens risk management, risk preparedness enhances crisis response, and institutional learning feeds back into strategic oversight. Through this recursive dynamic, cybersecurity leadership becomes a sustained capability that progressively strengthens long-term digital resilience and public confidence in educational institutions.

The six dimensions did not operate as static categories but emerged through a recursive governance internalisation process. Strategic governance integration triggered risk-informed decision-making, which subsequently shaped cultural reinforcement mechanisms. As awareness and cultural alignment matured, capability development became institutionalised. Crisis leadership episodes then tested the robustness of governance structures, often reinforcing ethical stewardship and executive accountability. This cyclical interaction suggests that cybersecurity leadership evolves through iterative reinforcement rather than linear progression. Figure 1 shows the Cybersecurity Leadership Model for Public Education Systems in Malaysia.

Figure 1: Cybersecurity Leadership Model for Public Education Systems in Malaysia.

When compared with the governance function in the NIST Cybersecurity Framework 2.0, the emergent model extends beyond compliance-based policy articulation by embedding executive identity transformation as a precursor to structured risk governance (Hossain et al., 2024).

FINDINGS

From Technical Delegation to Strategic Oversight

Across interviews, participants initially framed cybersecurity as an operational function delegated to ICT units, reinforcing a technical administrative boundary that insulated executive leadership from direct risk ownership. As one school principal explained:

"At first, we treated cybersecurity as something for the ICT teacher to handle. As long as the system was running and passwords were updated, we assumed everything was fine. It wasn't something discussed at management level." (Principal 3)

Similarly, a district-level officer noted:

"Cyber issues were considered technical problems. If there was a breach or system error, we called the ICT coordinator. It was not seen as part of strategic planning." (District Officer 2)

However, repeated exposure to cyber incidents and increasing policy mandates catalysed a perceptual and structural shift. A senior administrator reflected:

"After the ransomware incident, we realised this is not just an IT issue. It affects our reputation, student data, and even public trust. That's when it moved into our executive meetings." (Senior Administrator 1)

These accounts illustrate a process of organisational learning in which digital vulnerability became visible as systemic risk rather than technical anomaly. Cybersecurity leadership emerged when executive actors internalised digital risk as part of fiduciary and strategic accountability, marking a movement from delegated technical management to integrated governance stewardship.

Risk-Informed Decision-Making as Leadership Practice

Participants consistently link cybersecurity to decision-making under conditions of uncertainty. Leaders described balancing innovation pressures with risk accountability. A principal commented:

"We are encouraged to adopt new digital platforms, but now we ask: Where is the data stored? Who has access? What are the security implications? These questions were not asked before." (Principal 5)

A policy stakeholder elaborated:

"Every procurement decision now involves a risk discussion. It's no longer just about cost and functionality. We consider compliance, data protection, and long-term exposure." (Policy Officer 1)

Importantly, risk was framed not as technical probability but as governance judgement:

"If something goes wrong, it's not the ICT teacher who will answer to parents or the ministry. It's the school leadership. So the risk decision must sit at that level." (Principal 2)

These narratives demonstrate the institutionalisation of structured risk rationality within everyday leadership decisions. Rather than reactive crisis management, effective leaders normalised risk deliberation as part of strategic planning, reinforcing the co-constitutive relationship between transformation and protection.

Enacting A Cyber-Resilient Organisational Culture

Cybersecurity effectiveness was repeatedly described as dependent on behavioural norms and shared responsibility. One ICT coordinator observed:

"Even with firewalls and systems in place, if teachers click suspicious links, we are still vulnerable. Technology alone cannot protect us." (ICT Coordinator 4)

Leaders emphasised modelling behaviour:

"If I don't follow security protocols myself, how can I expect my staff to take it seriously? Leadership example is very important." (Principal 1)

However, awareness campaigns alone were insufficient:

"We used to send reminders about password changes, but people ignored them. Only when leadership consistently reinforced it in meetings did behaviour start to change." (District Officer 3)

These accounts illustrate the socio-technical character of cybersecurity leadership. Technological safeguards were necessary but insufficient without sustained cultural reinforcement. Institutions where leaders framed cybersecurity as shared governance responsibility demonstrated stronger adaptive responses and collective vigilance.

Capability Development and Distributed Governance

The findings reveal that cybersecurity leadership extended beyond individual authority to distributed capability. Participants described structured training and cross-department coordination as essential. A state-level officer noted:

"We realised that one person cannot carry cybersecurity alone. Training had to involve administrators, teachers, and support staff." (State Officer 1)

Similarly, the principal explained:

"We created a small committee to oversee digital risks. It includes the ICT coordinator, senior assistant, and discipline teacher. That way, responsibility is shared." (Principal 4)

Multi-level coordination emerged as critical:

"If schools don't communicate incidents to district level, patterns cannot be identified. Coordination across levels strengthens our overall response." (District Officer 1)

Where communication channels were unclear, vulnerability increased:

"Sometimes we assume someone else is handling it. That assumption creates gaps." (ICT Coordinator 2)

These findings demonstrate that cybersecurity leadership operated through governance alignment rather than hierarchical control alone. Capability development, policy clarification, and distributed accountability reduced fragmentation and strengthened institutional resilience.

The progression from initial codes to focused categories and the emergence of the core construction is summarised in Table 2. The table illustrates how recurring patterns in participants' accounts were abstracted into higher-level conceptual dimensions through constant comparison and memo analysis.

Table 2. Coding Progression from Initial Codes to Theoretical Dimensions

Core Category: Cybersecurity Leadership as Governance Integration	**Focused Category**	**Illustrative Initial Codes**	**Sample Participant Evidence**
Governance Internalisation Process	From Technical Delegation to Strategic Oversight	Delegating to ICT unit; excluding cyber risk from executive meetings; responding only after incidents; recognising reputational risk; including cybersecurity in budget planning	"At first, we treated cybersecurity as something for the ICT teacher to handle." (Principal 3)
		Translating technical breach into governance concern; discussing cyber risk at board level	"After the ransomware incident, it moved into our executive meetings." (Senior Administrator 1)
Risk Rationalisation in Leadership Practice	Risk-Informed Decision-Making	Balancing innovation and security; evaluating vendor data storage; considering compliance implications; accountability to stakeholders	"Now we ask where the data is stored and who has access." (Principal 5)
		Embedding risk review into procurement; reputational accountability	"It's not just about cost anymore. We consider long-term exposure." (Policy Officer 1)
Socio-Technical Cultural Reinforcement	Enacting a Cyber-Resilient Organisational Culture	Modelling secure behaviour; reinforcing password protocols; shifting from compliance reminders to governance framing; shared responsibility discourse	"Technology alone cannot protect us." (ICT Coordinator 4)
		Leadership example shaping behaviour; normalising vigilance	"If I don't follow security protocols, how can I expect my staff to?" (Principal 1)
Distributed Governance Alignment	Capability Development and Cross-Level Coordination	Establishing digital risk committees; conducting structured training; clarifying reporting channels; coordinating across school–district levels	"We created a small committee to oversee digital risks." (Principal 4)
		Preventing responsibility diffusion; formalising communication channels	"Sometimes we assume someone else is handling it. That assumption creates gaps." (ICT Coordinator 2)

Comparative cybersecurity policy studies across seven nations demonstrate that policy emphasis varies across attributes such as telecommunication governance, cloud infrastructure, identity protection, and digital signature regulation (Mishra et al., 2022). In contrast to decentralised governance environments where institutional autonomy drives cybersecurity adaptation, Malaysia's centralised bureaucratic structure shapes cybersecurity leadership through hierarchical policy transmission rather than autonomous local experimentation. Similarly, studies on local government cybersecurity policy highlight variability in policy comprehensiveness and formalisation (Hossain et al., 2024), suggesting that governance maturity strongly influences risk integration depth. The present model therefore reflects leadership enactment within a bureaucratically layered public

education system and may require adaptation in decentralised or federal education systems. These comparative insights provide a contextual backdrop for interpreting the theoretical implications of the present findings.

DISCUSSION

This study reconceptualises cybersecurity within public education as an executive governance competency rather than a peripheral technical or compliance function. In doing so, it addresses a structural gap within digital leadership scholarship, which has predominantly foregrounded innovation, digital maturity, and transformation capacity (Perifanis & Kitsios, 2023; Garcez et al., 2022; Aras & Büyüközkan, 2023), while under-theorising risk stewardship as a central leadership responsibility.

Across leadership tiers, cybersecurity was initially framed as an operational function delegated to ICT personnel. However, repeated exposure to cyber incidents and policy mandates catalysed a perceptual shift. Leaders increasingly recognised that digital risk implicated institutional reputation, data integrity, and public trust. This transition reflects what this study conceptualises as governance internalisation, the movement from technical delegation to executive ownership of digital risk.

While corporate governance research positions cybersecurity as a board-level responsibility (Alsulami, 2026), educational leadership theory has not fully incorporated this governance shift. The present findings demonstrate that, within public education systems, cybersecurity leadership emerges through integration into strategic planning, budgeting, procurement decisions, and cross-level coordination rather than through technical oversight alone.

When viewed alongside governance frameworks such as the NIST Cybersecurity Framework (Pham & Nguyen, 2023), the six-dimensional model aligns with structured categories of strategic context, risk management, policy articulation, and oversight. However, the contribution of this study lies not in replicating governance architecture but in explaining how governance becomes enacted.

Whereas formal frameworks specify what institutions should implement, the grounded model explains how leaders interpret, internalise, and operationalise those structures within bureaucratic systems. Cybersecurity leadership thus functions as a dynamic process linking strategy, culture, accountability, and crisis coordination rather than as a static compliance checklist.

The findings further reinforce socio-technical insights that cybersecurity effectiveness depends on behavioural norms, leadership modelling, and distributed awareness (Khadka & Ullah, 2025). Technical controls alone were consistently described as insufficient without sustained cultural reinforcement and cross-level accountability.

Simultaneously, the integration of crisis leadership and post-incident learning aligns the model with organisational resilience theory (Dahmen, 2023; Pradana & Ekowati, 2024). Cyber incidents were not only disruptions but catalysts for governance refinement and capability strengthening. Through recursive interaction among strategic oversight, risk rationalisation, cultural reinforcement, capability development, and ethical stewardship, cybersecurity leadership becomes a sustained adaptive capacity rather than a reactive response mechanism.

Unlike corporate environments characterised by market competition and decentralised authority, Malaysia's public education system operates within layered bureaucratic and regulatory structures. Consequently, cybersecurity leadership in this context is shaped by hierarchical policy transmission and distributed accountability rather than autonomous experimentation. This contextual grounding extends existing cybersecurity governance models, which are predominantly derived from private-sector settings (Savaş & Karataş, 2022).

While analytically portable, the model's enactment may differ in decentralised or market-oriented systems. Future comparative research is therefore necessary to examine how governance integration unfolds across diverse institutional architectures.

This study makes three primary contributions. First, it reframes cybersecurity as a governance construct embedded within executive leadership rather than a technical safeguard. Second, it provides a process-oriented explanation of how governance internalisation occurs across hierarchical levels within public education systems. Third, it integrates socio-technical systems and organisational resilience perspectives into digital leadership theory, thereby extending innovation-centric paradigms toward risk-informed governance. Together, these contributions reposition digital leadership as inherently tied to risk stewardship, ethical accountability, and institutional resilience in digitally intensive educational environments.

Limitations

While this study offers a substantively grounded model of cybersecurity leadership within public education, several limitations warrant careful consideration.

First, the study was conducted within Malaysia's public education system, which operates under a centralised governance structure characterised by layered bureaucracy, policy mandates, and hierarchical accountability. Although these structural features provided a rich context for examining governance integration, the findings may not fully capture leadership dynamics in decentralised or market-oriented education systems. Institutional autonomy, regulatory environments, and digital maturity levels vary significantly across national contexts. Consequently, while the Cybersecurity Leadership Model demonstrates analytical portability, its applicability beyond similarly structured public-sector systems should be assessed cautiously through comparative or cross-national studies.

Second, the research employed a constructivist grounded theory design based on 26 semi-structured interviews. Although theoretical saturation was achieved within the study's scope, the findings reflect participants' interpretive accounts rather than direct observational data. As with all qualitative research, the resulting theory is contextually situated and co-constructed through researcher–participant interaction. Future research may benefit from multi-method designs incorporating document analysis, policy audits, or incident case studies to triangulate leadership enactment across data sources.

Third, the study conceptualises cybersecurity leadership primarily through the lens of governance integration and risk stewardship. While this focus advances digital leadership theory beyond innovation-centric paradigms, it does not empirically measure institutional resilience outcomes or levels of digital trust. Quantitative validation studies could test the proposed model across larger samples, examining the relationships among governance integration, cultural reinforcement, crisis leadership, and measurable resilience indicators. Such work would strengthen generalisability and provide empirical assessment of the model's predictive utility.

Fourth, although participants represented multiple governance tiers, the sample was confined to public-sector actors. Private education institutions, international schools, and hybrid governance models may exhibit different risk rationalities and accountability structures. Expanding the model to alternative organisational forms would refine its boundary conditions and clarify contextual contingencies.

Finally, the rapid evolution of cyber threats and digital technologies presents a temporal limitation. Leadership practices observed during the study reflect current threat landscapes and regulatory expectations. As digital infrastructures become increasingly AI-integrated and data-intensive, cybersecurity governance responsibilities may evolve in scope and complexity. Longitudinal research is therefore needed to examine how cybersecurity leadership adapts over time in response to technological disruption and policy transformation.

Despite these limitations, the study provides a theoretically integrated and empirically grounded framework that advances understanding of cybersecurity as a core governance construct within educational leadership. By identifying governance internalisation, risk rationalisation, cultural reinforcement, and distributed alignment as interdependent mechanisms, the research establishes a foundation for subsequent empirical testing, comparative analysis, and policy development in digitally intensive educational systems.

CONCLUSION AND RECOMMENDATION

This study reconceptualises cybersecurity in public education from a predominantly technical or compliance-driven concern into a multidimensional leadership and governance construct. While prior scholarship has largely focused on infrastructure protection and user awareness (Afolalu & Tsoeu, 2025), governance research increasingly frames cybersecurity as an executive-level responsibility embedded within enterprise risk management and fiduciary oversight (Haque, 2025). Grounded in practitioner experiences across leadership, ICT coordination, and policy roles, the present findings demonstrate that cybersecurity in education is enacted through strategic prioritisation, policy alignment, risk ownership, crisis coordination, and ethical stewardship rather than through technical administration alone (Suleman et al., 2025).

By positioning cybersecurity as a core competency of digital-era leadership, the study advances educational leadership theory beyond innovation-centric paradigms that privilege agility and technological integration (Bozdağ, 2024; Gooderham et al., 2026). Instead, it embeds risk-informed decision-making within strategic governance structures and recognises cybersecurity as a structural condition shaping digital transformation trajectories (Mızrak, 2023). This reframing integrates ethical accountability in digitally intensive environments (Recker et al., 2025) and positions transformation and protection as co-constitutive rather than competing objectives.

Furthermore, by incorporating socio-technical systems theory and organisational resilience perspectives, the study underscores that cybersecurity effectiveness depends on the alignment of technical infrastructure, leadership behaviour, cultural norms, and adaptive learning processes (Hanafizadeh & Mehrasa, 2025; Ali, 2022; Isa et al., 2026). Cyber incidents are therefore reframed not merely as disruptions but as catalysts for governance refinement and institutional capability enhancement. Leadership operates as the coordinating mechanism linking risk oversight, behavioural reinforcement, crisis response, and institutional learning within a coherent governance architecture.

Although grounded in Malaysia's public education ecosystem, the Cybersecurity Leadership Model demonstrates analytical portability to other national systems navigating digital transformation under regulatory and accountability pressures (Adelusi et al., 2022; Devarajan et al., 2026). By integrating governance structures, cultural dimensions, risk management processes, and ethical stewardship within a unified explanatory framework, the study repositions cybersecurity as a strategic leadership domain and recalibrates digital leadership theory toward risk-conscious governance in digitally intensive educational environments.

ACKNOWLEDGEMENT

The researcher extends heartfelt gratitude to all the individuals who contributed to completing this research.

REFERENCES

1. Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2022). Advances in data lineage, auditing, and governance in distributed cloud data ecosystems. Shodhshauryam, International Scientific Refereed Research Journal, 5(4), 245-273.
2. Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. Future Internet, 17(12), 575.
3. Akkaya, B. (2023). Grounded theory: A comprehensive examination of data coding. International Journal of Contemporary Educational Research, 10(1), 89-103.
4. Ali, H. M., Ranse, J., Roiko, A., & Desha, C. (2022). Investigating organizational learning and adaptations for improved disaster response towards "resilient hospitals:" An integrative literature review. Prehospital and disaster medicine, 37(5), 665-673.
5. Ali, M. G. (2025). Cybersecurity Governance and Policy Development in Higher Education Institutions: A Strategic Framework for Resilience and Compliance. Online Submission.
6. Aras, A., & Büyüközkan, G. (2023). Digital transformation journey guidance: A holistic digital maturity model based on a systematic literature review. Systems, 11(4), 213.

7. Arora, A. (2025). Zero Trust Architecture: Revolutionizing Cybersecurity for Modern Digital Environments. Available at SSRN 5268151.
8. Assefa, E. A., & Mujtaba, B. G. (2025). Exploring transformational leadership in education by leveraging diversity and technology for inclusive practices. International Journal of Public Leadership, 21(4), 356-375.
9. Atasever, M., & Özen, E. (2025). The Relationship between Financial Information Security Management and Corporate Risk Management.
10. Bozdağ, A. A. (2024). Leadership Dynamics and Organizational Behavior in the Tech Industry: The Case of OpenAI. Journal of Organizational Behavior Review, 6(2), 158-186.
11. Barruga, M. B. (2025). Systematic Review Of Cybersecurity Frameworks For Higher Education Institutions: Characteristics, Components, And Challenges. International Journal of Applied Mathematics, 38(4s).
12. Bento, F., Adenusi, T., & Khanal, P. (2023). Middle level leadership in schools: a scoping review of literature informed by a complex system perspective. International Journal of Leadership in Education, 1-27.
13. Blown, E. J., & Bryce, T. G. (2022). When is an interview an inter view? The historical and recent development of methodologies used to investigate children's astronomy knowledge. Research in Science Education, 52(6), 1869-1908.
14. Bobbink, P., Larkin, P., & Probst, S. (2024). Application and challenges of using a Constructivist Grounded Theory methodology to address an undertheorized clinical challenge: A discussion paper. International journal of nursing studies advances, 6, 100199.
15. Bouncken, R. B., Czakon, W., & Schmitt, F. (2025). Purposeful sampling and saturation in qualitative research methodologies: recommendations and review. Review of Managerial Science, 1-37.
16. Bwiino, K., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2026). A Systematic Literature Review of Information Security Practices in Higher Education Contexts. IET Information Security, 2026(1), 6324508.
17. Chavarnakul, T., Xu, L. D., Bi, Z., Shankar, A., Dhiman, G., Viriyasitavat, W., & Hoonsopon, D. (2025). A Systematic Literature Review on Resilient Digital Transformation, Examining How Organizations Sustain Digital Capabilities. HighTech and Innovation Journal, 6(2).
18. Christodoulou, I. P., Rizomyliotis, I., Konstantoulaki, K., Alfiero, S., Hasanago, S., & Paolone, F. (2025). Investigating the key success factors within business models that facilitate long-term value creation for sustainability-focused start-ups. Business Ethics, the Environment & Responsibility, 34(3), 936-950.
19. Daher, W. (2023). Saturation in qualitative educational technology research. Education Sciences, 13(2), 98.
20. Dahmen, P. (2023). Organizational resilience as a key property of enterprise risk management in response to novel and severe crisis events. Risk Management and Insurance Review, 26(2), 203-245.
21. Devarajan, Y., Thandavamoorthy, R., Thatoi, D. N., Jangid, P. K., Manjunath, H. R., Zalawadia, J., ... & Mehar, K. (2026). Advancing SDG-7 for affordable and clean energy: decentralized energy access pathways, policy–finance barriers, and AI-enabled transition strategies. International Journal of Sustainable Energy, 45(1), 2620883.
22. Davidson, T., Wall, E., & Mace, J. (2023). A qualitative interview study of distributed tracing visualisation: A characterisation of challenges and opportunities. IEEE Transactions on Visualization and Computer Graphics, 30(7), 3828-3840.
23. Efe, A. (2025). Risk Modeling of Challenges and Opportunities in Harmonizing Traditional IT Governance with Emerging Cloud Governance Frameworks. Pamukkale Üniversitesi İşletme Araştırmaları Dergisi, 12(2), 411-435.
24. García-Nieto, M., Bueno-Rodríguez, V., Ramón-Jerónimo, J. M., & Flórez-López, R. (2024). Trends and risks in mergers and acquisitions: A review. Risks, 12(9), 143.
25. Garcez, A., Silva, R., & Franco, M. (2022). Digital transformation shaping structural pillars for academic entrepreneurship: A framework proposal and research agenda. Education and Information Technologies, 27(1), 1159-1182.
26. Gooderham, P., Schmeisser, B., Saebi, T., & Schotter, A. P. J. (2026). The digital transformation of international business: a conceptualization, multidisciplinary review, and research agenda. Journal of World Business, 61(1).
27. Hammar Chiriac, E., Forsberg, C., & Thornberg, R. (2023). Teachers' perspectives on factors influencing the school climate: A constructivist grounded theory case study. Cogent Education, 10(2), 2245171.
28. Hanafizadeh, P., & Mehrasa, S. (2025). Governance system design model in platform ecosystems by a socio-technical systems theory. Digital Policy, Regulation and Governance.

29. Haque, G. M. M., Akula, D. K., Mohammed, Y. S., Syed, A., & Arafat, Y. (2025). Cybersecurity risk management in the age of digital transformation: A systematic literature review. Emerging Frontiers Library for The American Journal of Engineering and Technology, 7(8), 126-150.
30. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding local government cybersecurity policy: A concept map and framework. Information, 15(6), 342.
31. Hossan, D., Wolfs, B., & Petkovic, M. (2025). Questionnaire validity and reliability: A review with practical guidelines. Journal of Entrepreneurship, Business and Economics, 13(1), 135-186.
32. Isa, R. A., Setiawan, B., & Pakaja, F. (2026). Cybersecurity awareness in the digital commerce ecosystem: factor analysis, program impact and future trends for consumers and MSMEs. Information & Computer Security, 1-26.
33. Iyer, S. S., & Raji, B. (2025). Cybersecurity culture and organizational resilience: A human-centered approach to digital risk management. American Journal of Industrial and Business Management, 15(5), 748-766.
34. Jalonen, H. (2025). A complexity theory perspective on politico-administrative systems: Insights from a systematic literature review. International Public Management Journal, 28(1), 1-21.
35. Kakar, Z. U. H., Rasheed, R., Rashid, A., & Akhter, S. (2023). Criteria for assessing and ensuring the trustworthiness in qualitative research.
36. Kamal, M. B., Hossain, M. B., Islam, J., Alam, I. K., Ibn Sayed, N., Assiri, M. A., & Mia, R. (2025). Digital ethics: A review of leadership theories, challenges, and responsibilities. Sage Open, 15(4), 21582440251386901.
37. Kesar, B. (2025). Impact of social media adoption on stakeholder engagement and trust. Management Matters, 1-29.
38. Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal: K. Khadka, AB Ullah. International Journal of Information Security, 24(3), 119.
39. Khan, M. I., & Khan, A. N. (2024). Exploring Management Practices and Theories through Grounded Theory: A Review. Journal of Policy Options, 7(3), 39-46.
40. Kin Heng, B. T., & Ng, M. Z. (2025). A Review of the Lifelong Learning and Continuing Education System in Singapore. Qualitative Report, 30(11).
41. Kouam, A. W. F. (2025). A systematic literature review of post-positivism and critical realism as epistemological frameworks in educational research. International Journal of Changes in Education, 2(2), 115-122.
42. 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.
43. Lian, Y., Deeprasert, J., & Jiang, S. (2025). Cognitive–Affective Negotiation Process in Green Food Purchase Intention: A Qualitative Study Based on Grounded Theory. Foods, 14(16), 2856.
44. Lim, W. M. (2025). What is qualitative research? An overview and guidelines. Australasian marketing journal, 33(2), 199-229.
45. Mehta, M., Pancholi, G., & Saxena, A. (2024). Organizational resilience and sustainability: a bibliometric analysis. Cogent Business & Management, 11(1), 2294513.
46. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, 102820.
47. Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management, 10(3), 98-108.
48. Musole, E. (2026). Embedding Ubuntu and Indigenous Business Insights in Zambia: Advancing a Neuro-Responsible Governance Framework for the Global South. International Journal of Advanced Business Studies, 5(1), 62-78.
49. Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 420-454.
50. Nguyen, L. T., & Tuamsuk, K. (2022). Digital learning ecosystem at educational institutions: A content analysis of scholarly discourse. Cogent Education, 9(1), 2111033.
51. Paapa, C., & Kambona, O. O. (2025). A critical review of grounded theory and thematic analysis in qualitative research: A way forward for qualitative Researchers. International Journal of Science and Research Archive, 16(3), 302-313.

52. Paigude, S. D., Pangarkar, S. C., Dari, S. S., Patil, M., & Gujar, S. N. (2024). A review of cybersecurity policies in the public sector: Challenges and solutions. Computer Fraud & Security, 2024(7), 7-12.
53. Perifanis, N. A., & Kitsios, F. (2023). Investigating the influence of artificial intelligence on business value in the digital era of strategy: A literature review. Information, 14(2), 85.
54. Pham, M. T., & Nguyen, L. H. (2023). A Comparative Review of Cybersecurity Standards and Frameworks: Supporting Information Assurance in Government and Industry Systems. Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems, 13(8), 1-15.
55. Pradana, D. W., & Ekowati, D. (2024). Future organizational resilience capability structure: a systematic review, trend and future research directions. Management Research Review, 47(10), 1586-1605.
56. Quainoo, C. R., & Ahad, M. A. R. (2026). The Role of Information Security in Responsible AI for Digital SMEs: A Systematic Review of Frameworks, Challenges, and Best Practices. Journal of Ethics and Emerging Technologies, 36(1), 1-29.
57. Qureshi, R., & Koo, I. (2026). A Comprehensive Survey of Cybersecurity Threats and Data Privacy Issues in Healthcare Systems. Applied Sciences, 16(3), 1511.
58. Recker, J., Chatterjee, S., Sundermeier, J., & Tarafdar, M. (2025). Digital responsibility: Current perspectives and future directions. Journal of the Association for Information Systems, 26(5), 1222-1238.
59. Reissner, S., & Whittle, A. (2022). Interview-based research in management and organisation studies: making sense of the plurality of methodological practices and presentational styles. Qualitative Research in Organizations and Management: An International Journal, 17(1), 61-83.
60. Safari, K., McKenna, L., & Davis, J. (2023). Promoting generalisation in qualitative nursing research using the multiple case narrative approach: a methodological overview. Journal of Research in Nursing, 28(5), 367-381.
61. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7-34.
62. Shava, G. N., Sibanda, S., Moyo, S., Bapire, K., & Mathonsi, E. (2022). Grounded Theory in Educational Research, Features and Processes a Review of Literature. International Journal of Research and Innovation in Social Science, VI, 811-818.
63. Soysal, Y., & Türkmen, S. (2024). Reinterpreting the member checking validation strategy in qualitative research through the hermeneutics lens. Qualitative Inquiry in Education: Theory & Practice, 2(1), 42-63.
64. Suleman, T. A., Okimiji, O. P., Atoro, T. K., & Adejo, J. E. (2025). Deployment of ChatGPT in Nigerian Universities: Addressing Research Challenges and Ethical Considerations. LASU Journal of Environmental Sciences, 1(1), 338-363.
65. Tharwat, H., Hafez, S. T., Elgohary, I. E., & Hassanein, A. (2025). A decade of cybersecurity research in internal auditing: bibliometric mapping and future research agenda. Discover Sustainability, 6(1), 1066.
66. Urquhart, C., Cheuk, B., Lam, L., & Snowden, D. (2025). Sense-making, sensemaking and sense making—A systematic review and meta-synthesis of literature in information science and education: An Annual Review of Information Science and Technology (ARIST) paper. Journal of the Association for Information Science and Technology, 76(1), 3-97.
67. Watini, S., Davies, G., & Andersen, N. (2024). Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments. International Transactions on Education Technology (ITEE), 3(1), 26-35.
68. Wendt-Lucas, N., Thomson Ek, H., Brynteson, M., & Jessen, S. (2025). Smart communities in the Nordic-Baltic region: a literature review: indicators and policies for bridging the urban-rural digital divide.
69. Wissemann, A. K., Pit, S. W., Serafin, P., & Gebhardt, H. (2022). Strategic guidance and technological solutions for human resources management to sustain an aging workforce: review of international standards, research, and use cases. JMIR Human Factors, 9(3), e27250.
70. Zamil, M. H., & Faruq, M. O. (2022). Cybersecurity And Data Integrity in Financial Systems: A Review Of Risk Mitigation And Compliance Models. International Journal of Scientific Interdisciplinary Research, 1(01), 27-61.