Developing A Cybersecurity Leadership Model for Educational Organizations in Malaysia: A Grounded Theory Study

Zul Afida Binti Abdullah[1], Rokiah Binti Mohd Nazir[2,] Kumaran Sekar[3] Shanti Ramanlingam PhD[4], Zizi'Azniza Binti Mohd[5], Roshafiza binti Hassan PhD[6]

[1,2,3,4]Department of Technology Development & Management centre National Institute of Educational Management & Leadership, Institute Aminuddin Baki, Malaysia.

[5]SMK Pelong, Terengganu

[6]University of Putra, Malaysia

DOI: https://dx.doi.org/10.47772/IJRISS.2026.10200139

Received: 11 February 2026; Accepted: 16 February 2026; Published: 26 February 2026

ABSTRACT

The digital transformation of education has intensified organizational dependence on connected platforms, cloud systems, and data-driven learning environments, thereby increasing exposure to cybersecurity risks such as ransomware, phishing, identity compromise, and data breaches. While educational cybersecurity research has predominantly focused on technical controls, cybersecurity in education is increasingly recognized as a leadership and governance challenge requiring institutional direction, cultural change, and strategic capabilitybuilding. In Malaysia, national initiatives such as MyDIGITAL, the Malaysia Education Blueprint (2013–2025), and the Digital Education Policy highlight the importance of digital readiness; however, there remains limited empirical understanding of how educational leaders enact cybersecurity leadership in complex organisational contexts. This study aims to develop a Cybersecurity Leadership Model for educational organizations in Malaysia, using grounded theory to capture leadership practices and governance mechanisms from practitioner perspectives. Semi-structured interviews were conducted with N=26 participants comprising education leaders, ICT coordinators, cybersecurity officers, and policy stakeholders across key educational settings. Data were analyzed through constant comparative analysis using open, axial, and selective coding, leading to the emergence of six core leadership dimensions such as strategic cyber governance, risk-informed decisionmaking, cyber-resilient culture and awareness, capability development and professional learning, incident leadership and crisis communication, and ethical compliance and data stewardship. The resulting model positions cybersecurity leadership as a socio-technical and governance-driven function that integrates institutional values with initiative-taking risk management and sustainable capacity-building. The study contributes a context-sensitive framework for guiding cybersecurity readiness and leadership development in Malaysia's educational ecosystem and offers actionable implications for leadership training institutions such as Institute Aminuddin Baki in strengthening cyber governance and organizational resilience.

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

INTRODUCTION

Education systems worldwide are undergoing accelerated digital transformation, characterized by widespread adoption of learning management systems, cloud services, educational analytics, remote learning applications, and integrated student information systems. While digitalization expands access and innovation, it also exposes educational institutions to expanding cybersecurity threats including ransomware attacks, credential theft, data breaches, and malicious exploitation of insecure networks (ENISA, 2023; OECD, 2023). Notably, education is consistently reported as a high-risk sector due to weak security maturity, limited technical resources, and high volumes of sensitive personal data (ENISA, 2023).

Cybersecurity is no longer purely an ICT technical matter. Instead, it increasingly represents a leadership problem involving organizational governance, resource allocation, decision-making under uncertainty, capability development, and ethical responsibility (von Solms & von Solms, 2018; Taddeo, 2017). Poor cybersecurity leadership results not only in technical failures but also in reputational damage, learning disruption, legal noncompliance, and public trust erosion (Bada & Nurse, 2019).

In Malaysia, education digitalization has expanded through national and ministerial initiatives including MyDIGITAL, the Malaysia Education Blueprint (2013–2025), and the Digital Education Policy. These policies emphasize digital competency, system transformation, and technology-enabled leadership. However, cybersecurity leadership remains under-theorized and insufficiently modelled specifically for educational organizational settings, where leadership roles span principals, district offices, ministry divisions, and training centers such as Institut Aminuddin Baki (IAB).

Problem Statement

Despite the rapid digitalization of educational systems worldwide, the education sector remains among the most vulnerable environments for cybersecurity threats, including phishing attacks, ransomware incidents, credential theft, unauthorized access to learning platforms, and large-scale leakage of sensitive student and staff data (ENISA, 2023; OECD, 2023). Educational organizations increasingly rely on interconnected digital ecosystems such as cloud services, learning management systems (LMS), online assessment tools, and administrative databases yet their cybersecurity readiness often lags their digital adoption. This imbalance creates significant exposure to cyber risks that can disrupt teaching and learning continuity, compromise institutional integrity, and diminish stakeholder trust, particularly among parents and communities.

Although cybersecurity threats are widely recognized, many educational institutions still respond to cybersecurity primarily through technical interventions, such as antivirus tools, firewall upgrades, password policies, or platform security settings. While these controls are necessary, contemporary research increasingly argues that cyber resilience depends not only on technology, but also on leadership behaviors, governance accountability, organizational culture, and decision-making processes (Bada & Nurse, 2019; von Solms & von Solms, 2018). In educational environments, cybersecurity failures frequently emerge from human and organizational factors such as low awareness, weak incident reporting practices, unclear accountability roles, limited budget prioritization, and inconsistent enforcement of digital policies across schools and administrative units. These issues indicate that cybersecurity is fundamentally a leadership challenge rather than purely an ICT function.

However, there is still limited empirical research that explains how educational organizations develop cybersecurity leadership capacity through governance mechanisms, cultural reinforcement, and system-wide capability development. Most existing cybersecurity frameworks and standards (e.g., cyber maturity frameworks and technical risk management models) emphasize technical risk controls and organizational compliance but provide inadequate guidance regarding how educational leaders should enact cybersecurity leadership, particularly across multi-level education systems where governance is distributed across ministries, state departments, district offices, and individual schools (ENISA, 2023; OECD, 2023). Consequently, there is a major research gap concerning what leadership looks like in cybersecurity contexts, how it is operationalized, and how it can be institutionalized as part of educational governance and leadership development.

In Malaysia, this gap becomes more critical due to the national push for digital transformation under initiatives such as MyDIGITAL, the Malaysia Education Blueprint (2013–2025), and the Digital Education Policy, all of which demand digitally competent and future-ready leadership. Yet the expansion of digital learning platforms and data-driven administration has created emerging cybersecurity risks within schools and educational agencies. For example, issues relating to data privacy of minors, unauthorized digital access, unsafe AI tool usage, and weak incident response readiness may occur without systematic leadership strategies to address them. Furthermore, cybersecurity responsibilities within the educational ecosystem often appear fragmented, where leaders may assume cybersecurity is the responsibility of ICT personnel, while ICT personnel may lack leadership authority, resulting in gaps in governance, coordination, and enforcement.

Importantly, Malaysia currently lacks a context-specific cybersecurity leadership model designed for educational organizations that aligns with the governance structure of the education system and supports leadership training and monitoring. A tailored model is needed to guide how cybersecurity leadership should be enacted across various levels, including the Ministry of Education (MOE), State Education Departments (JPN), District Education Offices (PPD), and schools. Such a model is also essential for institutional leadership training bodies such as Institute Aminuddin Baki (IAB) to strengthen leadership competencies in cybersecurity governance, risk-informed decision-making, resilience-building culture, and ethical data stewardship. Without a validated leadership model, cybersecurity initiatives may remain fragmented, reactive, and dependent on crisis-triggered responses rather than initiative-taking readiness planning and sustainable governance.

Therefore, this study addresses the pressing need to develop a Cybersecurity Leadership Model for Educational Organizations in Malaysia, grounded in stakeholder experiences and institutional contexts, to support strategic governance, continuous capacity building, and long-term organizational cyber resilience within the national education ecosystem.

Research Aim

This study aims to develop a cybersecurity leadership model for educational organizations in Malaysia. Specifically, it investigates how leaders and key stakeholders across the education system perceive and practice cybersecurity leadership, and how these real-world leadership practices can be synthesized into a grounded and context-relevant model. The study is significant because it contributes to the theoretical advancement of digital leadership and cyber governance in education, while also offering practical guidance for strengthening cybersecurity leadership at school and system levels. In addition, the findings will support the development of leadership competency training modules for Institute Aminuddin Baki (IAB) and Ministry of Education stakeholders and provide policy-aligned implementation strategies to enhance long-term cyber resilience across Malaysian educational institutions.

Research questions

RQ1: How do stakeholders across Malaysian educational organizations perceive cybersecurity risk and leadership responsibilities?

RQ2: What leadership practices and governance processes enable cybersecurity readiness and resilience in educational settings?

RQ3: How can these practices be integrated into a grounded cybersecurity leadership model suitable for system-wide implementation?

Significance of the study

This research contributes by:

1. Providing a grounded conceptualization of cybersecurity leadership in education
2. Producing a model relevant for IAB leadership development programs
3. Guiding JPN/PPD monitoring and school-level implementation
4. Supporting policy-aligned cyber governance capacity across MOE education system

Significance of Study

This study contributes to:

1. Theoretical advancement in digital leadership and cyber governance in education
2. Practical leadership guidance for educational organizations

3. Design of leadership competency training modules for IAB and MOE stakeholders

4. Policy-aligned implementation strategies to strengthen cyber resilience.

LITERATURE REVIEW

Cybersecurity Governance and Organizational Accountability

Cybersecurity governance refers to the institutional structures, leadership processes, and accountability systems that enable organizations to strategically manage cyber risks rather than responding reactively after incidents occur. Governance goes beyond technical security controls by clarifying who holds decision-making authority, how risks are prioritized, how cybersecurity resources are allocated, and how compliance is monitored across units and levels of leadership (OECD, 2023). In highly complex organizations such as education systems, cybersecurity governance is particularly important because responsibility is often distributed across multiple actors—leaders, administrators, ICT coordinators, vendors, and policy bodies. Without clear cybersecurity governance arrangements, organizations commonly experience role ambiguity where responsibilities remain undefined or overlapping, resulting in weak ownership of cyber risks, fragmented implementation, and delayed incident response (OECD, 2023).

Accountability is a core element of governance. Effective cybersecurity governance requires education organizations to develop clear policies, establish standard operating procedures, appoint responsible roles (e.g., cybersecurity focal persons), and integrate cybersecurity into institutional performance indicators and monitoring systems. This becomes increasingly critical as education institutions rely on cloud-based systems, digital learning platforms, and large-scale data ecosystems for student information management. Where accountability is weak, cybersecurity tends to become a technical issue delegated to ICT personnel without leadership authority, leaving organizational leaders disconnected from cyber risks and therefore less prepared to make urgent decisions during attacks or disruptions. Governance frameworks emphasize that cybersecurity readiness requires leadership ownership at the organizational level, including strategic oversight, policy compliance, risk review mechanisms, and continuous improvement practices (OECD, 2023). Thus, cybersecurity governance in education should be conceptualized not merely as ICT management, but as a strategic leadership function that ensures institutional stability and trust.

Human Behavior, Culture, and Awareness in Cybersecurity

While cybersecurity is often perceived as a technological domain, research consistently shows that a major portion of cyber incidents result from human and behavioral vulnerabilities. Staff members may unknowingly click malicious links, share passwords, reuse weak credentials, install unverified applications, or fail to report suspicious activities, thereby increasing organizational exposure to phishing, credential compromise, and data leakage (Bada & Nurse, 2019). The education sector is especially vulnerable due to high workforce diversity, different levels of digital literacy, and daily reliance on communication platforms such as email, messaging apps, and learning management systems. These behavioral risks highlight the critical role of organizational culture and awareness programs, particularly in environments where cybersecurity training is not embedded as routine professional development.

Cybersecurity culture refers to the shared values, practices, and behavioral norms that influence how individuals perceive and enact cyber-safe practices in daily work routines. Importantly, building cybersecurity culture is not achieved through one-off training programs. Instead, it requires ongoing reinforcement, leadership modelling, accessible reporting mechanisms, and organizational learning practices that reduce fear and blame (Bada & Nurse, 2019). Studies on cybersecurity awareness suggest that organizations with strong reporting culture and supportive leadership are more likely to detect threats early, respond quickly, and reduce the impact of incidents. In contrast, blame-driven cultures often discourage staff from reporting phishing attempts or mistakes, allowing vulnerabilities to remain hidden until a major breach occurs.

Therefore, cybersecurity culture is fundamentally a leadership responsibility. Leaders must communicate that cybersecurity is a shared duty, normalize incident reporting, and ensure staff are empowered to recognize and

respond to threats. Within educational organizations, school leaders and system administrators must also guide teachers and staff in safe practices, particularly because education involves vulnerable populations such as children and minors, where safety breaches can cause significant harm. Thus, organizational cybersecurity culture should be treated as a central pillar in cybersecurity leadership, requiring continuous awareness campaigns, trust-based reporting systems, and behavioral accountability embedded into the education system.

Leadership and Risk-Informed Decision-Making

Cybersecurity leadership requires leaders to engage in complex decision-making under uncertainty. Unlike technical decisions that can be delegated to ICT personnel, cybersecurity incidents often demand quick organizational-level responses: deciding whether to shut down systems, how to communicate with stakeholders, how to preserve evidence, and how to restore operational continuity. Risk-informed decision-making involves the ability to interpret risks, evaluate potential impacts, prioritize controls, and make trade-offs that balance organizational goals with cybersecurity protection. In educational contexts, leaders frequently face trade-offs between keeping learning systems accessible and implementing stricter security measures that might disrupt teaching and learning operations.

The concept of cybersecurity as risk governance highlights that cyber risks should be integrated into routine strategic leadership decisions rather than being treated as a rare crisis event (von Solms & von Solms, 2018). From this perspective, cybersecurity leaders must operate as risk managers who promote institutional resilience through proactive planning, policy enforcement, and continuous monitoring. When leaders lack cyber literacy, decision-making tends to become reactive, based on uncertainty or dependence on external advice, weakening organizational response speed and effectiveness. This is particularly significant in the education ecosystem because school leaders may not be trained in cybersecurity decision-making, and education governance systems may not provide consistent cyber risk dashboards or maturity indicators to guide leadership actions.

Thus, cybersecurity leadership in education requires leaders to develop cognitive and strategic competencies for risk interpretation, prioritization, and decision-making under constraints such as limited budgets and human capacity. Risk-informed decision-making is increasingly essential as cyber threats become more frequent, sophisticated, and unpredictable, making it critical for education leaders to integrate cyber risk management into strategic planning, operational governance, and leadership accountability systems (von Solms & von Solms, 2018).

Ethical Compliance and Protection of Minors' Data

Cybersecurity in education has unique ethical dimensions because education organizations manage highly sensitive data particularly the personal and academic records of minors. Unlike many corporate settings, educational data breaches can have long-term negative consequences for children's identity security, privacy, and well-being. Cyber incidents in schools can disrupt learning environments and generate public concern, especially when sensitive student data is exposed. Therefore, cybersecurity leadership in education must prioritize ethical compliance, responsible data stewardship, and transparent governance practices to maintain public trust and uphold the moral obligations of educational institutions.

Ethical frameworks for digital transformation emphasize key principles such as transparency, fairness, accountability, and human-centered system design (UNESCO, 2021). In educational contexts, this means leaders must ensure that cybersecurity decisions protect vulnerable groups and prevent harm, rather than focusing purely on operational convenience. Furthermore, as schools increasingly adopt AI-powered tools and analytics systems, ethical risks expand beyond cyberattacks to include misuse of personal data, unauthorized sharing of student records, and adoption of digital tools without sufficient understanding of data storage and privacy implications. Floridi et al. (2022) emphasise that responsible digital governance requires human-centered and value-aligned leadership, ensuring that technology supports social good rather than amplifying inequality or creating harm.

Therefore, cybersecurity leadership in education must incorporate ethical digital governance as a central dimension. Leaders handle ensuring compliance with data protection requirements, strengthening institutional transparency during incidents, and guiding safe adoption of emerging digital tools. In Malaysia, where education

reforms are closely tied to national digital strategies, ethical compliance becomes even more crucial to ensure that innovation aligns with public trust, student protection, and national governance standards.

Research Gap: Limited Model Development for Cybersecurity Leadership in Malaysia's Education Ecosystem

Although cybersecurity leadership research is expanding globally, most studies remain grounded in corporate, financial, or national defense contexts, where leadership structures, accountability systems, and operational environments differ significantly from educational institutions. Many cybersecurity frameworks prioritize technical maturity, compliance checklists, or risk modelling, offering limited insight into the leadership processes and governance practices required to sustain cybersecurity readiness across a multi-level education system. In education systems like Malaysia, cybersecurity governance involves multiple layers MOE, JPN, PPD, leadership training institutions such as IAB, and individual schools each with distinct responsibilities, authority boundaries, and resource limitations.

Despite Malaysia's rapid education digitalization, there is limited empirical evidence on how cybersecurity leadership is enacted across these governance levels and how leadership capability can be developed systematically through training and monitoring mechanisms. As a result, Malaysia lacks a context-specific, education-tailored cybersecurity leadership model that captures governance complexity, cultural challenges, incident readiness needs, and ethical stewardship obligations. This gap is significant because without a leadership model, cybersecurity efforts may remain fragmented, reactive, and uneven across schools and districts.

Given these limitations, grounded theory is particularly appropriate because it supports the development of a model rooted in stakeholder experiences, institutional realities, and socio-technical environments (Charmaz, 2014). A grounded model can find how cybersecurity leadership is perceived and practiced across different governance actors, and how leadership dimensions interrelate to produce cyber resilience. Therefore, this study responds directly to the research gap by developing an empirically grounded cybersecurity leadership model that aligns with Malaysia's education governance ecosystem and supports IAB's leadership development mandate.

METHODOLOGY

This study employed a qualitative research design using constructivist grounded theory to generate a cybersecurity leadership model grounded in stakeholder experiences and institutional realities within Malaysia's educational governance ecosystem (Charmaz, 2014).

A total of 26 participants were recruited through purposive sampling followed by theoretical sampling, enabling the study to include information-rich stakeholders across multiple governance levels, including Institut Aminuddin Baki (IAB) senior trainers and instructional designers, school principals and senior assistants, school ICT coordinators, District Education Office (PPD) officers, State Education Department (JPN) ICT/administration officers, MOE-linked policy and cybersecurity stakeholders, and cybersecurity/IT risk practitioners supporting educational agencies.

Data were collected through semi-structured interviews lasting 45 to 90 minutes, which allowed participants to share in-depth insights into cybersecurity risks, governance and accountability mechanisms, organizational capability and readiness, incident response practices, and ethical challenges relating to student data and the increasing use of AI tools in education.

Data analysis followed the constant comparative method, a hallmark of grounded theory, involving open coding to identify initial concepts, axial coding to build relationships among categories, and selective coding to integrate categories into a central explanatory process that formed the final grounded model (Charmaz, 2014; Glaser & Strauss, 1967). Trustworthiness and methodological rigor were enhanced through established qualitative quality procedures including member checking, peer debriefing, maintenance of audit trails, and the use of thick description to strengthen credibility, dependability, and confirmability (Lincoln & Guba, 1985; Creswell & Poth, 2018).

FINDINGS

Overview of Emergent Categories

The grounded theory analysis revealed six interconnected cybersecurity leadership dimensions across Malaysian educational organizations. These dimensions emerged consistently from stakeholder perspectives at multiple governance levels (MOE, JPN, PPD, schools, and IAB). Overall, participants described cybersecurity leadership not as a technical task but as a governance-driven leadership responsibility requiring structured accountability, risk-informed decision-making, sustained capability development, and ethical stewardship of sensitive student data. The six emergent categories were: (1) strategic cyber governance and accountability, (2) risk-informed decision-making and prioritization, (3) cybersecurity culture and behavioral reinforcement, (4) capability development and professional learning ecosystems, (5) incident leadership and crisis communication, and (6) ethical compliance and data stewardship. Together, these categories represent the foundation for building systemic cyber resilience within Malaysia's education ecosystem.

Open Coding Table

During, interview transcripts were analyzed line-by-line to identify repeated meanings, actions, and perceptions. Each excerpt was condensed into a first code describing leadership patterns, governance weaknesses, cultural barriers, and readiness issues. These open codes were later grouped into broader categories during axial coding.

Table 1: summary of open coding outcome

Raw interview excerpt	**Open code**	**Brief explanation of meaning**
"Cyber only becomes serious when there is a crisis."	reactive leadership	Leaders prioritize cybersecurity only after incidents occur, not proactively.
"We do not know who should approve incident escalation."	accountability ambiguity	Reporting lines and authority structures are unclear across school/PPD/JPN.
"Teachers worry reporting is seen as incompetence."	fear-based silence	Staff avoid reporting incidents due to fear of blame or reputation loss.
"Training is once a year, but threats change monthly."	training misalignment	Cyber training is not continuous; content is outdated and infrequent.
"Parents ask: was my child's data leaked?"	trust & reputational risk	Cyber incidents create parental anxiety and damage public trust.
"Sometimes the ICT teacher becomes the cybersecurity person without appointment."	informal cyber role assignment	Cyber tasks are assigned informally without clear competency or recognition.
"We have circulars, but no one checks implementation."	weak enforcement monitoring	Policies exist but are not monitored through audits/KPIs.
Raw interview excerpt	**Open code**	**Brief explanation of meaning**
"If MOE says block website today, schools struggle to comply tomorrow."	policy–practice implementation gap	System directives do not match school capacity and resources.
"School leaders depend on vendors, but vendors don't understand education needs."	over-reliance on external support	Lack of internal capability forces dependence on external ICT vendors.
"Leaders worry about disruption, so security controls are delayed."	operational continuity priority	Leaders focus on maintaining school operations even if security risk remains.

"When ransomware happens, we panic because no one has practiced the SOP."	lack of incident simulation	Crisis procedures are theoretical, not rehearsed or internalized.
"Teachers use AI tools for lesson plans; they paste student information unknowingly."	uncontrolled data exposure via AI	AI use increases privacy risks due to poor awareness of data boundaries.

Summary of open coding outcome

Theme 1: Strategic Cyber Governance and Accountability

Findings strongly indicate that cybersecurity leadership within Malaysian educational organizations is fundamentally shaped by the strength of strategic governance and accountability mechanisms. Participants across the governance ecosystem (MOE, JPN, PPD, IAB, and schools) emphasized that cybersecurity readiness depends less on the availability of technology and more on whether institutions have clear governance structures that define leadership roles, responsibilities, and enforcement systems. In many schools, cybersecurity responsibilities were described as informally assigned to ICT coordinators or "tech-savvy" teachers, even though these individuals often lacked official authority to enforce cyber policies or influence procurement and system-wide decision-making.

Consequently, principals were positioned as the ultimate organizational leaders facing cyber risk, yet without adequate governance support, monitoring structures, or cybersecurity decision-making frameworks. This governance gap resulted in fragmented practices where cybersecurity initiatives lacked ownership and continuity across different education levels. As one district-level leader explained, diffusion of responsibility often leads to ineffective implementation:

"Cybersecurity is everyone's responsibility, but because of that it becomes no one's responsibility." (P07).

Similarly, school leaders reported that operationalizing cybersecurity procedures remains difficult, despite the presence of standard documents, because the procedures are not translated into practical school-level workflows:

"The SOP exists, but in school context we do not know how to operationalize it." (P02).

Three major governance-related subthemes emerged. First, role definition across system levels was repeatedly raised as a critical weakness, particularly regarding who should lead and approve cyber actions during incidents, procurement decisions, or compliance reporting. Second, participants stressed the importance of cybersecurity KPIs, audits, and monitoring mechanisms to ensure policies are not only disseminated but also practiced consistently. Participants argued that governance without monitoring promotes "paper compliance" rather than cyber readiness. Third, leaders highlighted that cybersecurity maturity requires budget prioritization and procurement governance, as schools cannot implement cyber improvement without financial planning and system-level support. Overall, this theme shows that strategic cyber governance is a central pillar of cybersecurity leadership and a prerequisite for systematic cyber resilience.

Theme 2: Risk-Informed Decision-Making and Prioritization

The second theme highlights cybersecurity leadership as a process of risk-informed decision-making, where leaders must interpret cyber threats, prioritize institutional actions, and manage trade-offs under real constraints. Participants explained that leaders often face uncertainty when balancing cybersecurity requirements with the need to maintain learning continuity and school operations.

In practice, cybersecurity decisions were frequently described as being delayed or simplified because many leaders lacked confidence in evaluating risk severity and selecting the most appropriate mitigation strategies. A cyber practitioner explained that weak risk understanding results in leadership delays, increasing vulnerability exposure:

"When leaders do not understand risk, they delay decisions." (P10).

Similarly, school leaders acknowledged that operational pressures sometimes push them toward convenience driven choices rather than structured risk prioritization:

"Sometimes we choose convenience because we must keep teaching." (P14).

These findings reflect how cyber risk leadership in education is often constrained by limited expertise, limited time, and competing organizational priorities.

Three related subthemes were identified. First, cyber literacy among leaders emerged as essential because leadership decision-making requires foundational understanding of cyber risks even if leaders are not technical experts. Participants suggested that principals and senior assistants require competency in cyber governance and risk interpretation, particularly regarding data breaches, phishing risks, and escalation decisions. Second, participants emphasized the need for prioritization tools, such as cyber risk dashboards or maturity indicators, that enable evidence-based leadership decisions across MOE–JPN–PPD–school levels. Third, leaders highlighted a constant tension between decision speed and evidence constraints, where leaders must act quickly during cyber incidents even without full technical certainty. Therefore, this theme positions cybersecurity leadership as an evolving capability that integrates risk thinking into daily governance routines rather than treating cybersecurity only as a technical emergency.

Theme 3: Cybersecurity Culture and Behavioral Reinforcement

Theme three indicates that cybersecurity readiness in education is significantly shaped by organizational culture, especially staff behavior patterns, incident reporting norms, and psychological safety. Participants reported that even when policies and tools are available, cybersecurity risks remain high due to human factors, particularly weak reporting culture and fear-driven avoidance. A major barrier was described as a blame culture, where staff worry that making mistakes such as clicking phishing links will be treated as incompetence or negligence. This fear leads to silence, under-reporting, and delayed detection of cyber threats. An ICT coordinator clearly summarized the type of culture that leaders must promote:

"If teachers report phishing, do not punish them thank them." (P15).

In addition, a state-level stakeholder emphasized the importance of moving from reactive fear to proactive resilience: *"The culture must shift from fear to readiness."* (P19).

These findings show that cybersecurity leadership is closely tied to the ability of leaders to influence behavior and norms, making culture-building a central leadership function.

Three subthemes explain how cyber culture is strengthened. First, trust-based reporting culture is required so staff feel safe reporting incidents, near-misses, or vulnerabilities without fear of punishment. Participants indicated that early reporting prevents larger breaches and builds organizational learning. Second, leaders described the need for continuous awareness strategies, noting that one-off cyber briefings are insufficient due to rapidly evolving threats. Effective culture requires repeated messaging, reminders, and contextual learning. Third, reinforcement mechanisms were identified as important leaders should reward cyber-safe behavior, acknowledge proactive staff actions, and normalize learning from mistakes. This theme reinforces that cyber resilience depends on leadership-driven culture where safety behaviors become shared responsibility across the institution.

Theme 4: Capability Development and Professional Learning Ecosystems

The fourth theme emphasizes that cybersecurity leadership requires sustainable and structured capability development, extending beyond technical training to include leadership competencies, operational readiness, and system-level professional learning. Participants consistently argued that cyber resilience cannot be achieved through isolated or annual training programs.

Instead, cybersecurity competence must be developed continuously through structured professional learning ecosystems aligned across governance levels. Participants shared that many cybersecurity workshops are either

too technical, too general, or not tailored to role expectations in schools, resulting in low transfer into practice. An IAB trainer captured this need for role-based leadership training: *"Principals need cyber decision-making skills, not technical coding."* (P03).

A national-level stakeholder further supported continuous learning, likening cyber readiness to emergency preparedness: *"Our capacity building should be continuous like fire drills."* (P08). Overall, this theme shows that cybersecurity leadership maturity is dependent on continuous institutional learning and capacity development embedded in leadership training systems.

Three subthemes emerged. First, participants highlighted the need for competency mapping and development pathways, ensuring different roles (principals, senior assistants, clerks, teachers, ICT coordinators) receive tailored cyber leadership and operational skills. Second, simulation-based learning was strongly recommended, including tabletop exercises, mock phishing drills, and cyber incident simulations to strengthen readiness and confidence. Third, participants stressed the importance of coaching and communities of practice, where peer networks and continuous support structures enable sustained competency. This theme demonstrates how IAB plays a strategic role, as it can institutionalize cybersecurity leadership competency development as part of national education leadership programs.

Theme 5: Incident Leadership and Crisis Communication

Theme five highlights cybersecurity incidents as high-stakes organizational crises requiring effective incident leadership, rapid escalation, and structured crisis communication. Participants reported that cyber incidents create intense pressure for leaders to act quickly while ensuring correct reporting, evidence preservation, service continuity, and transparent stakeholder communication. A critical issue raised was that while SOPs exist at system level, many leaders lack confidence in implementing them operationally in school contexts due to limited practice and unclear escalation lines.

A cyber officer emphasized that leadership communication can significantly influence organizational response: *"During an incident, leadership communication determines whether panic spreads."* (P21).

Meanwhile, a district officer explained that unclear escalation structures can promote concealment of incidents rather than transparency: *"Without clear escalation lines, people hide issues."* (P16). This theme suggests that incident readiness is not only technical; it is shaped by leadership ability to coordinate crisis responses and manage communication professionally.

Three incident leadership subthemes were identified. First, participants emphasized crisis SOPs and escalation protocols, including who reports to whom, what actions to take, and how to coordinate across agencies (PPD,

JPN, MOE). Second, participants highlighted continuity of learning operations, where leaders must protect school functions while controlling cyber threats. Third, communication protocols to parents and media were identified as essential to maintain trust and avoid misinformation. This theme demonstrates that effective cyber incident leadership requires structured governance, crisis readiness training, and communication competencies.

Theme 6: Ethical Compliance and Data Stewardship

The final theme demonstrates that cybersecurity leadership in education carries a strong dimension of ethical responsibility and data stewardship, particularly because educational organizations manage minors' data. Participants emphasized that safeguarding student information is not only a compliance requirement but a moral duty. A policy stakeholder summarized this clearly:

"Children's data is not like ordinary data there is a moral duty." (P09).

Participants further highlighted emerging ethical risks due to increasing adoption of AI tools in schools. Staff sometimes use AI platforms for teaching materials or administrative tasks without recognizing that data may be stored externally or processed beyond institutional control.

As one ICT specialist noted: *"Sometimes teachers upload documents into AI tools without understanding where data goes."* (P26).

These findings show that cybersecurity leadership now overlaps with ethical governance, requiring institutions to regulate digital practices, especially in relation to data privacy and AI usage.

Three subthemes emerged. First, leaders identified the need for a strong data protection culture, where ethical safeguarding becomes institutional norms rather than optional practice. Second, participants stressed compliance monitoring, arguing that schools require structured supervision mechanisms, not informal reminders. Third, ethical AI usage emerged as a growing priority, requiring boundaries, guidelines, and governance structures to prevent misuse, data leakage, and breaches of privacy. Overall, this theme positions cybersecurity leadership as value-driven leadership protecting students, maintaining trust, and ensuring responsible innovation.

Model Development: CSL-EdMY

This study developed the Cybersecurity Leadership Model for Education Malaysia (CSL-EdMY) through selective coding, which integrated all themes into one central (core) category: governance-driven organizational cyber resilience. This core category explains that cybersecurity leadership in educational organizations is not only technical, but primarily a leadership and governance function that strengthens resilience through structured accountability, risk-based decision-making, continuous capability building, positive cybersecurity culture, effective incident leadership, and ethical data stewardship. The CSL-EdMY model conceptualizes cybersecurity leadership as a system consisting of inputs, core leadership dimensions, and outcomes. The inputs include national digital policies, the complexity of multi-level educational governance (MOE–JPN–PPD–schools), and the evolving cyber threat environment. These drivers shape six core leadership dimensions, which collectively influence key outcomes, namely improved cyber readiness maturity, reduced incident recurrence, faster response and recovery, and stronger public trust and system integrity.

Von Solms & Von Solms (2018) cybersecurity positioning and governance importance

DISCUSSION

Findings show that cybersecurity leadership in education is less about technical mastery and more about governance capability and organizational resilience. The CSL-EdMY model reinforces contemporary arguments positioning cybersecurity as a leadership and socio-technical system challenge (OECD, 2023; von Solms & von Solms, 2018).

The model further expands cybersecurity literature by demonstrating that education requires multi-level governance alignment and monitoring across school leadership and administrative agencies, resonating with ENISA's (2023) concern about education sector vulnerabilities. Additionally, the ethical compliance dimension highlights unique education-sector responsibility regarding minors' data, aligning with ethical AI and digital governance principles (Floridi et al., 2022; UNESCO, 2021).

Implications

The findings of this study provide important implications for strengthening cybersecurity leadership and governance across Malaysia's educational ecosystem. For Institut Aminuddin Baki (IAB), the CSL-EdMY model offers a structured and evidence-based framework that can be embedded into leadership development programs to improve cybersecurity readiness among school leaders and education officers.

IAB can operationalize the model by introducing competency-based modules on strategic cyber governance and accountability, implementing risk-informed decision-making simulations that reflect realistic school cyber scenarios, and strengthening leaders' crisis readiness through incident response and crisis communication training. In addition, IAB may consider developing an ethical digital leadership certification, which equips leaders with strong competencies in data privacy, responsible technology adoption, and ethical use of AI tools in educational settings.

At the system level, the implications extend to the Ministry of Education (MOE), State Education Departments (JPN), and District Education Offices (PPD), particularly in ensuring coordinated governance and monitoring. These agencies can improve national cybersecurity readiness by establishing a clear system-wide accountability matrix that defines cybersecurity roles and decision-making authority across governance levels. Moreover, implementing cyber maturity dashboards and monitoring KPIs would support evidence-based supervision and reduce uneven implementation across schools. Finally, the standardization of incident escalation protocols is essential to ensure cyber incidents are managed efficiently with clear reporting lines, faster response coordination, and reduced disruption to teaching and learning operations.

CONCLUSION

This grounded theory study developed CSL-EdMY, a cybersecurity leadership model specifically tailored to the Malaysian educational ecosystem. The model conceptualizes cybersecurity leadership as governance-driven organizational cyber resilience, highlighting that cybersecurity readiness in education is not solely dependent on technical safeguards but is strongly shaped by leadership practices, accountability structures, organizational culture, continuous capability development, crisis readiness, and ethical data stewardship. CSL-EdMY provides both a meaningful theoretical contribution to digital leadership and cyber governance scholarship, and a practical leadership tool that can support training, policy implementation, and system-wide monitoring across MOE, JPN, PPD, IAB, and schools to strengthen long-term cybersecurity resilience in Malaysian education.

REFERENCES

1. Argyris, C., & Schön, D. A. (1996). Organizational learning II: Theory, method, and practice. AddisonWesley.
2. Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programs for small-and-medium-sized enterprises (SMEs). Information and Computer Security, 27(3), 393–410.
3. Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. Interacting with Computers, 23(1), 4–17.

4. Charmaz, K. (2014). Constructing grounded theory (2nd ed.). SAGE Publications.
5. Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.
6. Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. Business Research, 13, 215–246.
7. ENISA. (2023). ENISA threat landscape 2023. European Union Agency for Cybersecurity.
8. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2022). AI4People.An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707.
9. Glaser, B. G., & Strauss, A. L. (1967). The discovery of grounded theory: Strategies for qualitative research. Aldine.
10. Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Ashgate.
11. ISO. (2018). ISO 31000:2018 risk management—Guidelines. International Organization for Standardization.
12. Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.
13. OECD. (2023). Cybersecurity policy-making in the education sector: An overview. OECD Publishing.
14. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. UNESCO Publishing.
15. von Solms, R., & von Solms, S. (2018). Cybersecurity and information security—What goes where? Information & Computer Security, 26(1), 2–9.