Global Journal of Computer Science and Technology - Section G
GJCST

The Cybersecurity Governance Gap in Ecuadorian SMEs: IT–Management Alignment, Decision Rights, and Incident-Response Accountability

Franklin Orellana[ϑ *]

ϑ Doctor of Business Administration, Master of Business Administration, Master of Information Technology

Abstract

Cybersecurity weaknesses in small and medium-sized enterprises (SMEs) are frequently attributed to limited budgets, inadequate training, and obsolete technology. This explanation is incomplete when employees responsible for cybersecurity recognize risks but lack the authority, executive access, and governance routines needed to convert that knowledge into organizational action. This article presents a governance-centered secondary analysis of documentary evidence from a 2020 qualitative study of 50 information technology and cybersecurity managers working in Ecuadorian SMEs. The corpus comprised anonymized participant quotations, thematic tables, and narrative findings preserved in the dissertation. Guided by business–IT strategic alignment and the Govern function of the National Institute of Standards and Technology Cybersecurity Framework 2.0, the analysis identified five interconnected mechanisms: responsibility without decision authority, weak translation of cyber risk into business priorities, fragmented communication and escalation, resource allocation disconnected from risk ownership, and limited monitoring and organizational learning. Negative cases showed that periodic audits, stakeholder monitoring, and direct owner–IT collaboration can partially counter these constraints. The article contributes a resource-sensitive Cybersecurity Governance Alignment Model in which incident-response capability depends on aligning accountability, decision rights, communication, resources, and monitoring. For SME managers, the study proposes a minimum viable governance cycle that can be implemented without enterprise-scale bureaucracy.

Keywords: *Business–IT Alignment, Cybersecurity Governance, Decision Rights, ecuadorian smes, Emerging Economies, Enterprise Risk Management, Incident Response, NIST Cybersecurity Framework*

*** Corresponding Author**
Franklin Orellana

1. Introduction

Small and medium-sized enterprises depend increasingly on cloud services, digital payments, remote access, mobile devices, and data-intensive operations. This dependence expands business opportunity while making operational continuity inseparable from cybersecurity. Yet SMEs generally possess fewer specialized personnel, smaller technology budgets, and less formal governance than large enterprises. Research consistently shows that smaller firms struggle to implement balanced cybersecurity capabilities across identification, protection, detection, response, and recovery [1, 2, 3, 4].

Technical controls alone do not explain this condition. Cybersecurity decisions are organizational decisions: leaders define priorities, allocate budgets, accept risk, authorize changes, assign responsibility, and determine what information reaches senior management. When cyber responsibility is delegated to an IT employee, but authority remains centralized with an owner or general manager, the employee can become accountable for outcomes without being empowered to acquire tools, train personnel, enforce procedures, or escalate risk. This misalignment creates a governance gap.

The National Institute of Standards and Technology (NIST) made governance explicit in Cybersecurity Framework (CSF) 2.0. The Govern function establishes organizational context, risk strategy, roles, responsibilities, authorities, policy, oversight, and supply-chain risk management as foundations for the other five functions [5]. NIST's small-business guide similarly stresses that leaders must understand priorities, assign authority, and integrate cyber risk into broader business decisions [6]. Incident-response guidance now treats preparation and response as components of continuing cyber-risk management rather than isolated technical activity [7].

This governance perspective is especially important in emerging economies, where firms may operate through centralized ownership, informed procedures, limited specialist labor markets, and uneven public support. Prior work based on Ecuadorian SMEs identified cultural, readiness, leadership, and return-on-security-investment barriers [8, 9]. However, the earlier article synthesized those barriers broadly; it did not isolate the internal governance mechanism through which recognized cyber risks fail to become authorized and resourced action.

The purpose of this article is therefore to explain how IT management alignment, decision rights, communication, resource allo-

cation, and monitoring shape incident-response accountability in Ecuadorian SMEs. The article addresses three research questions:

- **RQ1:** How do SME IT managers describe the alignment between cybersecurity responsibility and managerial authority?
- **RQ2:** Which governance and communication mechanisms impede the conversion of recognized cyber risk into incident-response action?
- **RQ3:** What minimum governance configuration can resource-constrained SMEs use to improve incident-response accountability?

The study contributes to a Cybersecurity Governance Alignment Model that moves beyond a list of barriers. The model explains incident-response capability as an outcome of five mutually reinforcing governance functions: strategic translation, decision rights and accountability, resource allocation, communication and escalation, and monitoring and learning.

2. Materials and Methods

2.1. SME cybersecurity as an organizational problem

SME cybersecurity research has expanded, but much of it remains concentrated on threats, awareness, and protective controls. Chidukwani, Zander, and Koutsakis found that SME research was disproportionately focused on the Identify and Protect functions of the earlier NIST framework, with less attention to Detect, Respond, and Recover [1]. Their later empirical work likewise emphasized the need to validate what firms report against operational evidence [2]. Studies in different national settings show that resource constraints interact with managerial priorities, internal capabilities, regulation, and access to expertise rather than operating as independent causes [3, 10].

Cyber-organizational resilience research reinforces this socio-technical interpretation. Neri and Niccolini found that Italian SMEs frequently lacked structured planning and post-event learning, while awareness, resources, and firm size constrained resilience practices [4]. In Ecuador and the wider Latin American region, institutional capacity, workforce development, digital infrastructure, and cross-sector collaboration remain important contextual conditions [11, 12]. These findings suggest that SME weakness is not reducible to the absence of a specific firewall or training session. The central problem is how technical knowledge and organizational authority are coordinated.

2.2. Business–IT strategic alignment

Strategic alignment concerns the degree to which business strategy, organizational infrastructure, IT strategy, and IT processes reinforce one another. Henderson and Venkatraman established alignment as a continuing organizational process rather than a one-time technology decision [13]. Luftman later operationalized alignment maturity through communication, competency and value measurement, governance, partnership, scope and architecture, and skills [14]. These dimensions are directly relevant to cybersecurity because cyber risk crosses business, technology, legal, financial, operational, and reputational boundaries.

In an aligned SME, the individual responsible for cyber operations understands business priorities, managers understand material cyber dependencies, decision rights are explicit, security expenditures are evaluated through risk and business value, and results are reviewed. In a misaligned SME, IT personnel may recognize threats but cannot translate them into managerial action; leaders may demand accountability without delegating authority; and security decisions may occur only after a disruption.

2.3. Governance, accountability, and incident response

Cybersecurity governance provides direction and oversight for cyber-risk management. ISO/IEC 27001:2022 requires an information security management system that is established, implemented, maintained, and continually improved in the organization's context [15]. NIST CSF 2.0 similarly treats governance as the means through which risk strategy, responsibility, authority, policy, and oversight guide operational outcomes [5]. These standards do not require SMEs to reproduce large-enterprise bureaucracy. They require clarity about who decides, who acts, what gets reported, and how performance is reviewed.

Clear accountability is ineffective when it is not paired with authority. A person tasked with protecting systems must be able to escalate incidents, obtain defined resources, require essential controls, and convene the people needed for response. Conversely, managers who retain decision authority must receive intelligible risk information and accept ownership of residual risk. Governance therefore connects the technical and business sides of incident response.

The conceptual framework used here integrates business–IT alignment with NIST CSF 2.0 governance outcomes. Five analytical dimensions were defined: (1) strategic translation of cyber risk into business consequences; (2) alignment of accountability and decision authority; (3) risk-based resource allocation; (4) communication and escalation across hierarchical levels; and (5) monitoring, assurance, and learning. These dimensions guided the secondary analysis.

3. Results

3.1. Research design and provenance

This article uses a qualitative secondary documentary analysis of evidence reported in Orellana's 2020 doctoral dissertation [8]. The original exploratory study collected open-ended electronic questionnaire responses through SurveyMonkey from 50 participants identified principally as IT managers and cybersecurity managers associated with Ecuadorian SMEs. Participants were recruited through professional LinkedIn contacts. The dissertation reports that responses were coded with NVivo 12 and organized around two questions concerning cyberattack response protocols and ROI/ROSI-related response practices.

No new participants were recruited for the present article. The analytical corpus was limited to anonymized participant quotations, thematic tables, code descriptions, and narrative findings preserved in the fourth and fifth chapters of the dissertation. The present analysis does not claim access to interview recordings, Zoom transcripts, MAXQDA files, or demographic details that are not documented in the dissertation. This boundary is important because the 2025 publication contains methodological descriptions that should be reconciled against original records before any future raw-data reanalysis [9].

3.2. Distinction from the 2025 publication

The 2025 article examined cybersecurity readiness, cultural dynamics, leadership, ROSI, resistance to change, and external collaboration [9]. The current article asks a narrower and different question: how governance alignment affects the conversion of cyber-risk knowledge into authorized incident-response action. It

EARLY REVIEW

Table 1. Provenance and analytical differentiation

Element	2020 dissertation	2025 article	Current article
Primary focus	Response protocols and ROI/ROSI practices	Broad readiness, culture, leadership, ROSI, and collaboration	Governance alignment, decision rights, and accountability
Evidence base	50 open-ended electronic questionnaires; reported themes and quotations	Dataset described as supporting broad qualitative analysis	Documentary corpus preserved in dissertation chapters IV–V
Framework	Hofstede, McClelland, and dialectical theory	Cultural and leadership frameworks	Business–IT alignment and NIST CSF 2.0 Govern
New contribution	Original exploratory findings	Culturally adaptive readiness synthesis	Mechanism-based Cybersecurity Governance Alignment Model

applies a new conceptual framework, reorganizes the dissertation evidence into new governance mechanisms, includes negative-case analysis, and develops new tables and a new model. It does not reproduce the earlier article's five-theme synthesis, results structure, or recommendations.

3.3. Analytical procedure

A directed qualitative content-analysis procedure was used. First, all reported quotations and thematic descriptions relevant to management support, authority, communication, budgeting, technology acquisition, staffing, protocols, auditing, asset monitoring, and learning were identified. Second, evidence was provisionally coded against the five conceptual dimensions. Third, inductive subcodes were created when the evidence expressed a mechanism not adequately captured by the initial labels. Fourth, evidence within and across themes was compared to distinguish symptoms—such as missing tools—from governance causes—such as absent authority or risk ownership. Fifth, negative or deviant cases were examined, including participants who described auditing, stakeholder monitoring, owner–IT collaboration, or no need for change.

Code frequencies reported in the dissertation are presented only as characteristics of the original qualitative analysis. They are not treated as population estimates, causal effects, or statistically generalizable prevalence. Quotations are attributed using the dissertation's anonymized participant labels. The present interpretations distinguish empirical evidence from the later normative mapping to NIST CSF 2.0, which postdates the original data collection.

3.4. Ethical and quality considerations

The dissertation reports institutional approval, informed consent, anonymization, and procedures intended to protect participant confidentiality [8]. The current article analyzes only de-identified evidence already included in the dissertation. Credibility was strengthened through an explicit provenance table (Table 1), a theory-informed code structure, comparison of supporting and contradictory evidence, and conservative claim boundaries. Before journal submission, the author should confirm the original consent and institutional requirements, data-retention status, publisher rights, and the fidelity of English translations to the original Spanish responses.

4. Discussion

The governance-centered reanalysis produced five interconnected themes (summarized in Table 2). These themes do not imply that every SME displayed the same configuration. Instead, they identify recurring mechanisms through which recognized cybersecurity needs were separated from organizational authority and action.

4.1. Responsibility without decision authority

Participants frequently described responsibility for cyber protection without corresponding authority over budgets, staffing, training, or policy enforcement. The original RQ1 analysis identified stakeholder support as a distinct component of SME challenges, while the dissertation's seventh table placed stakeholder support alongside technology and education [8]. The quotations clarify the mechanism: IT employees understood gaps but were unable to cross hierarchical boundaries.

> *"I really would love to have more support from our top managers and to have more interaction with them, but it seems there is a huge wall between them and the employees."* **— Participant A22 [8]**

The "wall" is an alignment failure. Technical responsibility resides below the level at which strategic and financial authority is exercised. Participant A45 similarly connected absent management support to reduced IT performance, while Participant A6 described personnel as having their "hands tied" without management-sponsored training. Accountability in this configuration is asymmetric: IT staff may be blamed for vulnerabilities while lacking authority to change the conditions producing them.

4.2. Weak translation of cyber risk into business priorities

A second mechanism was the inability to translate cybersecurity into terms that competed successfully with immediate revenue and operating priorities. Participant A5 explained that the general manager was focused on making money and did not treat the IT function as comparably important. Participant A39 attributed weak attention to response protocols to an owner's limited understanding of technology. These statements indicate more than low awareness. They reveal a translation gap between technical vulnerability and business exposure.

> *"I hope our top manager understands the importance of cybersecurity and how this can impact the organization. The current owner of the company does not understand much about the technology industry."* **— Participant A39 [8]**

When cyber risk is communicated primarily as a request for equipment or training, managers may interpret it as discretionary cost. Alignment requires expressing the operational process at risk, plausible loss scenario, decision deadline, proposed control, residual risk, and accountable owner. The dissertation's ROSI evidence reinforces this problem: participants reported limited ability to monitor assets or explain whether security investments were producing expected value.

EARLY VIEW

Table 2. Governance mechanisms identified in the secondary analysis

Mechanism	Illustrative dissertation evidence	Operational consequence	Governance requirement
Responsibility–authority mismatch	"Huge wall" between managers and employees; "hands tied" without sponsorship	Recognized risks do not become authorized controls	Assign decision rights, escalation authority, and accountable risk owners
Business–cyber translation gap	Revenue priority; limited owner technology understanding	Security remains a discretionary IT cost	Translate risk into service, financial, legal, and continuity consequences
Fragmented communication	Requests for meetings, interaction, training, and direction	Unclear preparation, escalation, and learning	Establish recurring cyber-risk reviews and incident communication rules
Unowned investment monitoring	No one monitoring assets/investments; uncertainty about ROSI	Limited budgets cannot be prioritized or evaluated	Maintain asset/risk register, treatment owner, metric, and review date
Emergent positive governance	Periodic audits, stakeholder monitoring, owner–IT list of measures	Partial structure despite limited size	Use lightweight assurance and direct owner–IT collaboration

4.3. Fragmented communication, escalation, and cross-functional routines

The evidence also showed that communication occurred episodically rather than through defined governance routines. Participants requested more meetings, more interaction with managers, monthly training, and clearer direction. Participant A43 reported that managers and owners barely met with IT employees to explain how the organization was moving. The dissertation's fifth chapter explicitly identified weak communication between general management and network or cybersecurity administrators [8].

Without a scheduled risk review, documented escalation threshold, or cross-functional incident role, cybersecurity remains isolated within IT. This isolation matters before, during, and after an incident. Before an incident, risk acceptance remains implicit. During an incident, authority to disconnect systems, communicate with customers, obtain outside assistance, or interrupt operations may be unclear. After an incident, lessons may not become approved changes.

4.4. Resource allocation disconnected from risk ownership and monitoring

Budget limitations were real, but the evidence indicated a governance problem beyond scarcity. Participants described missing ownership for tracking security investments, inadequate asset inventories, and uncertainty about whether ROSI analysis was performed correctly. Participant A45 called for someone to monitor IT investments, and Participant A16 requested management software to monitor technology and investments. The absence of ownership and measurement makes it difficult to prioritize even a limited budget.

> *"Our company does not have someone monitoring the IT investment. We need to have someone who starts tracking this and check what the best return of investment scenario for the company is."* **— Participant A45 [8]**

Risk-based allocation requires a minimum information base: critical assets and services, responsible owners, plausible incident scenarios, control costs, expected loss reduction, and review dates. Without these elements, requests for technology compete as isolated purchases rather than components of an approved risk-treatment plan. This helps explain why participants simultaneously requested tools, specialists, training, and stronger protocols without a coordinating governance mechanism.

4.5. Negative cases: signs of workable governance

Not every account described complete inaction. Participant A41 reported periodic IT audits intended to confirm whether ROSI was met, and Participant A43 described stakeholders monitoring antivirus investments and server updates. Participant A33 stated that, despite lacking a security team, employees worked with the owner to maintain a list of measures for protecting company information. These cases are limited and do not establish mature governance, but they show that direct owner engagement, assigned monitoring, and recurring assurance can partially compensate for organizational size.

The negative cases also clarify the difference between governance and bureaucracy. A small firm does not necessarily require a board committee, full-time chief information security officer, or complex reporting system. It requires explicit decisions, named owners, routine communication, evidence of implementation, and a learning loop.

5. Discussion

5.1. Cybersecurity readiness as an alignment outcome

The findings show that readiness is not only a stock of tools, skills, or procedures. It is an alignment outcome. An SME may employ an IT manager who recognizes phishing, outdated systems, weak backups, or inadequate firewalls; yet response capability remains weak if the individual cannot secure executive attention, obtain authorization, coordinate departments, or monitor implementation. This distinction extends earlier work that described broad readiness and cultural barriers in Ecuadorian SMEs [9].

Business–IT alignment theory helps explain why the observed deficits co-occurred. Communication, governance, partnership, value measurement, architecture, and skills are interdependent [14]. The dissertation evidence displayed the same interdependence: participants asked for training, tools, qualified professionals, management support, process improvement, and investment monitoring. Treating each request separately obscures the governance configuration needed to make the components effective.

5.2. The Cybersecurity Governance Alignment model

Figure 1 presents the resulting model. Incident-response capability is positioned as the outcome of five aligned governance functions. Strategic translation connects threats to business services and consequences. Decision rights and accountability establish who accepts risk, who authorizes action, and who executes it. Resource allocation connects limited funds to prioritized risk treatment. Communication and escalation ensure that material information crosses hierarchical and functional boundaries. Monitoring and

EARLY VIEW

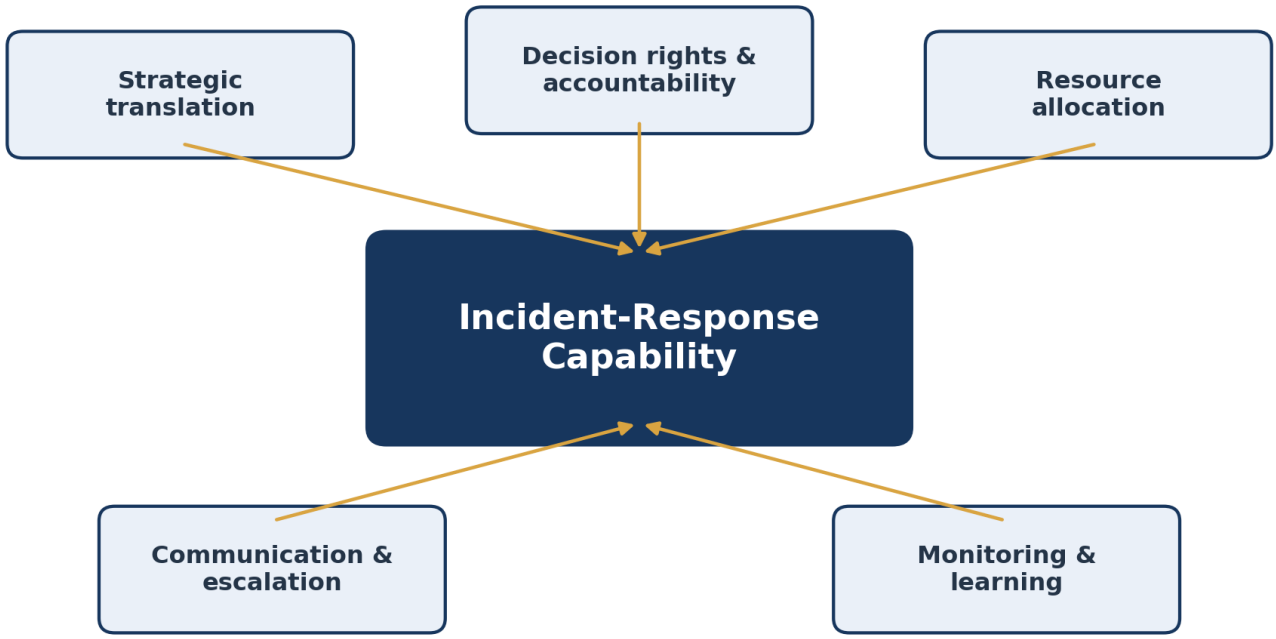


Figure 1. Cybersecurity Governance Alignment Model for resource-constrained SMEs.

learning verify implementation and convert incidents, exercises, and audits into improvement.

The model is consistent with NIST CSF 2.0, but it is not a retroactive compliance assessment. The 2020 participants were not evaluated against a framework published in 2024. Rather, CSF 2.0 provides a current normative vocabulary for interpreting why authority, roles, policy, oversight, and risk strategy matter. The qualitative evidence explains how governance outcomes can fail in practice.

5.3. Minimum viable governance for SMEs

The findings support a minimum viable governance cycle that does not depend on enterprise-scale staffing:

- **Define context:** Identify the three to five business services whose disruption would create the greatest operational, financial, legal, or reputational harm.
- **Assign ownership:** Name a business risk owner, a technical response lead, an alternate, and the person authorized to accept residual risk.
- **Set escalation rules:** Define which events require owner/executive notification, outside assistance, customer communication, legal review, or service shutdown.
- **Prioritize treatment:** Maintain a short risk register connecting assets, scenarios, controls, costs, owners, deadlines, and residual risk.
- **Review quarterly and after events:** Examine control status, incidents, near misses, training, supplier issues, and unresolved decisions; document actions and owners.
- **Exercise annually:** Conduct a short scenario-based tabletop exercise and revise roles, contact information, backups, communications, and recovery priorities.

This cycle reframes cybersecurity from an IT request into a recurring management process (Table 3). Its value is not the production of documents; it is the creation of explicit, reviewable decisions.

Table 3. Minimum viable cybersecurity governance routine

Routine	Owner	Minimum evidence	Suggested cadence
Business-service and risk review	Owner/general manager with IT lead	Prioritized services, scenarios, risk owners, accepted residual risk	Quarterly
Asset and control review	IT lead/process owners	Critical asset list, backup status, access review, unresolved vulnerabilities	Monthly or quarterly
Incident escalation check	Incident lead and management	Current contacts, decision thresholds, external support, communication authority	Quarterly
Tabletop exercise	Management, IT, operations, communications	Scenario, decisions, gaps, assigned corrective actions	Annually
Post-incident learning review	Business owner and response lead	Timeline, impact, decisions, lessons, corrective actions, completion evidence	After every material incident

6. Contributions and Implications

6.1. Scholarly contribution

This article makes three contributions. First, it reframes SME incident-response weakness as a governance alignment problem rather than a simple shortage of awareness, tools, or money. Second, it identifies mechanisms connecting hierarchical separation to operational capability: authority–accountability mismatch, weak strategic translation, fragmented escalation, and unowned monitoring. Third, it develops a resource-sensitive model that links business–IT alignment to contemporary cybersecurity governance without assuming large-firm structures.

The findings also add emerging-economy evidence to a literature dominated by North American, European, and Australasian contexts. The Ecuadorian evidence suggests that managerial centralization and informal processes can make direct owner–IT alignment especially consequential. Future comparative research should test whether the model operates differently across family-owned firms, sectors, cities, and Latin American countries.

6.2. Managerial implications

For owners and general managers, the principal implication is that delegating cyber tasks does not delegate cyber risk. Executives retain responsibility for priorities, authority, resources, and risk acceptance. They should require concise risk reporting while giving the technical lead defined authority to escalate and implement approved controls. For IT managers, technical requests should be translated into business-service impact, plausible loss, decision options, costs, and residual risk. For advisors and policymakers, templates and training should address governance conversations and decision routines, not only employee awareness or control checklists.

6.3. Implications for standards and education

SME guidance based on NIST CSF 2.0 or ISO/IEC 27001 should be localized into a small number of observable management practices. Training programs should include owner cyber literacy, risk communication, incident decision-making, and after-action learning. This need aligns with evidence that Latin America continues to face cybersecurity workforce and capability constraints [11]. Universities and professional associations can contribute by offering bilingual scenario-based programs that place business leaders and IT personnel in the same exercise.

7. Limitations and Future Research

Several limitations constrain the conclusions. The underlying evidence was collected for a 2020 dissertation and reflects conditions at that time. The original sample was purposive, relied on self-reported open-ended questionnaires, and was overwhelmingly private sector. The present study analyzed quotations, thematic displays, and narrative findings preserved in the dissertation rather than the complete raw response archive. Translation procedures and some methodological descriptions should be verified against original records. Code frequencies are not population estimates, and the design cannot establish causality.

Future research should collect paired evidence from SME owners and IT managers to measure perceptual alignment, compare stated governance with documentary and operational evidence, and test the proposed model. A mixed-method design could examine whether clarity of decision rights, risk-review cadence, management cyber literacy, and exercise participation predict incident-response maturity. Longitudinal research should evaluate whether implementation of the minimum governance cycle improves time to escalate, corrective-action completion, backup recovery performance, and investment decision quality. Cross-country studies could determine how regulation, trust, infrastructure, and national business culture moderate the model.

8. Conclusions

Ecuadorian SME cybersecurity cannot be strengthened solely by purchasing tools or instructing employees to be more aware. The dissertation evidence shows that people responsible for security often recognized the necessary actions but lacked management access, authority, resources, and monitoring structures. The resulting governance gap separated technical knowledge from organizational decision-making.

The Cybersecurity Governance Alignment Model explains incident-response capability as the product of five aligned functions: strategic translation, decision rights and accountability, resource allocation, communication and escalation, and monitoring and learning. A minimum viable governance cycle can bring these functions together without imposing enterprise-scale bureaucracy. The essential shift is from treating cybersecurity as an isolated IT expense to governing it as an ongoing business risk and resilience responsibility.

Data Availability and Related-Publication Disclosure

This article is a secondary documentary analysis of anonymized evidence reported in Orellana's 2020 doctoral dissertation [8]. The dissertation dataset also informed a 2025 article addressing broad cybersecurity readiness, culture, leadership, ROSI, and collaboration [9]. The present article asks a distinct governance-alignment question, applies a different conceptual framework, and presents new analysis, tables, figures, and conclusions. No new participant data were collected for this article. Any future analysis of original raw records should proceed only after confirming consent, institutional requirements, retention status, and data integrity.

PARTIAL VIEW

RESEARCH FIELD

Franklin D. Orellana: Cybersecurity governance; SME risk management; IT–business alignment; incident response; organizational resilience; Latin American cyber policy; qualitative research; data governance; digital transformation.

REFERENCES

[1] Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, 10, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

[2] Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses. *Computers & Security*, 145, 104026. https://doi.org/10.1016/j.cose.2024.104026

[3] Hoong, Y., & Rezania, D. (2024). Balancing talent and technology: Navigating cybersecurity and privacy in SMEs. *Telematics and Informatics Reports*, 15, 100151.

[4] Neri, M., & Niccolini, F. (2025). On the path to cyber organizational resilience: Shedding light on the context of SMEs. *International Journal of Organizational Analysis*, 33(12), 105–131. https://doi.org/10.1108/IJOA-06-2024-4572

[5] National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

[6] National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide* (NIST SP 1300). https://doi.org/10.6028/NIST.SP.1300

[7] Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61r3). https://doi.org/10.6028/NIST.SP.800-61r3

[8] Orellana, F. D. (2020). *Cybersecurity incident response capabilities in the Ecuadorian small business sector: A qualitative study* [Doctoral dissertation, Northcentral University].

[9] Orellana, F. (2025). Assessing cybersecurity response readiness and return on security investment strategies among SMEs in Ecuador. *Global Journal of Computer Science and Technology*, 25(G1), 27–33. https://doi.org/10.34257/GJCSTGVOL25IS1PG27

[10] De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, 141, 103826. https://doi.org/10.1016/j.cose.2024.103826

[11] OECD. (2023). *Building a skilled cyber security workforce in Latin America: Insights from Chile, Colombia and Mexico*. OECD Publishing. https://doi.org/10.1787/9400ab5c-en

[12] Inter-American Development Bank & Organization of American States. (2020). *Cybersecurity: Risks, progress, and the way forward in Latin America and the Caribbean*. https://doi.org/10.18235/0002513

[13] Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), 4–16.

[14] Luftman, J. (2000). Assessing business–IT alignment maturity. *Communications of the Association for Information Systems*, 4, Article 14. https://doi.org/10.17705/1CAIS.00414

[15] International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*.

[16] Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

EARLY VIEW