

Embedding Cybersecurity Governance into Corporate Planning: A Framework for Mid-Market Philippine Logistics Firms

Victor P. Claveria¹ , Jean V. Ramos² 

Author Information:

¹Cloud Synergy Logistics, Inc., Silang, Cavite, Philippines

²Graduate School, University of Luzon, Dagupan City, Pangasinan, Philippines

Correspondence: vpclaveria17@gmail.com

Article History:

Date Received: September 7, 2026

Date Revised: September 10, 2026

Date Accepted: October 8, 2026

Date Published: October 14, 2026

DOI: <https://doi.org/10.67903/ijroms0482>

Document ID: 2026IJROMS0482

Recommended Citation:

Claveria, V. P. & Ramos, J. V. (2026). Embedding Cybersecurity Governance into Corporate Planning: A Framework for Mid-Market Philippine Logistics Firms. *International Journal of Research on Multidisciplinary Studies*, 1(9), 323–336. <https://doi.org/10.67903/ijroms0482>

Abstract. Cybersecurity governance is increasingly framed as a planning-stage function embedded in resource-allocation and approval processes rather than as a downstream technical control. This shift has progressed furthest in banking, while mid-market third-party logistics (3PL) providers remain largely outside the discussion despite handling sensitive client data and maintaining deep application programming interface (API) integrations with enterprise clients. Prior studies typically offer either standardized extent-of-practice measurement or contextual explanation, rarely both, leaving unclear how extensively cybersecurity governance is integrated into corporate planning and why integration varies across similar firms. This study addressed this gap through a convergent mixed-method multi-case design involving five purposively selected, anonymized Philippine logistics firms. A structured 20-item survey, adapted from the Govern function of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0 and the Control Objectives for Information and Related Technologies (COBIT) 2019, measured integration across four dimensions (Governance Structure, Risk Management Integration, Policy Formalization, and Resource Allocation) among 35 personnel, while key informant interviews and document reviews provided contextual explanations. The survey demonstrated good internal consistency ($\alpha = .83$). Firms with both client-facing integrations and formal senior-level governance oversight (Firms C and D) were classified as “substantially integrated” (3.85 and 3.63), while firms lacking both (Firms A and E) were classified as “minimally integrated” (2.20 and 2.35). Resource Allocation received the highest scores and Policy Formalization the lowest, suggesting that digital investment has outpaced formal governance practices. Interviews indicated that higher-scoring firms converted triggering events into established planning practices through senior-level governance oversight, whereas lower-scoring firms treated cybersecurity primarily as a responsibility of information technology contractors. The study proposes a four-layer framework (Governance, Planning-Gate, Risk-Integration, and Resource-Alignment) and recommends that industry associations develop a voluntary, sector-specific governance benchmark.

Keywords: Governance Integration; Policy Formulation; Resource Allocation; Risk Management; Third-Party Risk

Introduction

Cybersecurity has moved from the server room to the boardroom over the past decade, and international standards now describe this shift explicitly instead of leaving it as an implicit trend. The National Institute of Standards and Technology (NIST) formalized this change in 2024 through CSF 2.0, adding an entirely new “Govern” function to what had been a five-function technical framework, signaling that accountability, risk appetite, and oversight are now core to cybersecurity practice, not an afterthought layered on top of it (NIST, 2024). Regulators and enterprise clients alike have followed this logic outward from the largest, most exposed organizations toward the vendors and partners connected to them: the financial sector has absorbed this change fastest, embedding cyber risk into board reporting and regulatory examination, and global supply-chain data now shows why that pressure keeps spreading further downstream, with a large and rising share of major breaches traced back to a third party rather than the organization itself (International Business Machines Corporation, 2024; World Economic Forum & Accenture, 2024). Governance, in other

words, is no longer confined to the firms large enough to be regulated directly; it increasingly follows the data and the system connections wherever they lead.

Mid-market third-party logistics and freight-forwarding firms in the Philippines sit squarely in that downstream position, and yet remain almost entirely outside the frame of existing research and regulation. These firms operate inside the supply chains of the enterprise clients they serve, hold sensitive shipment and customs data, and increasingly connect to client systems through application programming interfaces, extending each client's own attack surface into the 3PL firm's systems in the process. They are not subject to a supervisory framework comparable to that established by BSP Circulars 808 and 982 for Philippine banks, and limited empirical research has examined cybersecurity governance among Philippine 3PL firms. This creates a governance blind spot precisely where digital exposure is accelerating fastest. This study addresses that blind spot by asking how far cybersecurity governance has actually been integrated into the corporate planning processes of five mid-market Philippine 3PL firms, and, just as importantly, why that integration varies so widely from one firm to the next despite the firms sharing a common industry and client base.

Research Questions

This study aimed to determine the extent to which cybersecurity governance is integrated into the corporate planning processes of mid-market Philippine third-party logistics (3PL) and freight-forwarding firms, examine the factors that account for variations in such integration across firms, and propose a framework to support the systematic integration of cybersecurity governance into corporate planning.

Specifically, this study seeks to answer the following questions:

1. What is the extent of cybersecurity integration as a corporate planning function among mid-market Philippine logistics firms in terms of:
 - 1.1 Governance Structure;
 - 1.2 Risk Management Integration;
 - 1.3 Policy Formalization; and
 - 1.4 Resource Allocation?
2. How does the extent of cybersecurity–corporate planning integration vary across the five case firms in relation to firm size, years in operations, and the presence of enterprise API/system integrations with clients?
3. What factors explain differences in cybersecurity governance integration into each case firm's corporate planning process?
4. What patterns emerge from the integration of quantitative and qualitative findings across the five case firms?
5. What model can be developed from the integrated findings to embed cybersecurity governance into corporate planning among mid-market Philippine logistics firms?

Scope and Delimitation of the Study

The scope of this study covered the integration of cybersecurity governance into corporate planning among mid-market third-party logistics (3PL) and freight-forwarding firms in the Philippines across four dimensions: Governance Structure, Risk Management Integration, Policy Formalization, and Resource Allocation. Five purposively selected firms (Firms A–E) were included, representing differences in firm size, years of operation, and enterprise API or client-system integration. Data were collected from 35 personnel in planning, executive, finance, and IT roles through a structured survey, key informant interviews, and internal document review. Mid-market firms were defined as locally incorporated 3PL and freight-forwarding providers employing approximately 25–350 personnel, above micro and small enterprise thresholds but below multinational or publicly listed logistics companies. The study focused on the integration of cybersecurity into governance and planning processes rather than the technical effectiveness of security controls; therefore, penetration testing, vulnerability scanning, and technical security audits were not included. The five firms were selected through purposive maximum-variation sampling, so the findings are intended for analytic rather than statistical generalization. Excluded from the study: clients, regulators, and third-party vendors, none of whom were directly surveyed or interviewed, along with foreign-headquartered firms operating only through Philippine branches. The study used a cross-sectional design, assessing cybersecurity integration at a single point in time, and drew its survey primarily from the NIST Cybersecurity Framework (CSF) 2.0 Govern function and selected COBIT 2019 governance and management objectives. Technical control maturity and workforce cybersecurity literacy were not part of it. The findings therefore focus on how cybersecurity governance is integrated into corporate planning and the factors influencing this integration across the five participating Philippine 3PL firms.

Literature Review

Cybersecurity Governance as a Planning-Stage Function

Cybersecurity was traditionally viewed as a technical responsibility, with security controls typically implemented after systems were developed and managed primarily by information technology departments, with limited involvement from senior executives responsible for budgets and strategic decisions. Von Solms and van Niekerk (2013) describe the evolution of this perspective by distinguishing “information security,” historically centered on protecting the confidentiality, integrity, and availability of information, from “cybersecurity,” which encompasses the broader protection of an organization’s people, processes, and strategic interests from threats that extend beyond the direct control of IT. This broader perspective positions cybersecurity as an enterprise risk comparable to financial and operational risk, making it an important consideration in organizational planning and decision-making. International governance frameworks reflect this development. NIST’s Cybersecurity Framework (CSF) 2.0, released in February 2024, introduced the Govern function as a sixth core function alongside the five functions established in earlier versions. It emphasizes organizational context, cybersecurity strategy, oversight responsibilities, and policy, reinforcing the role of senior leadership in managing cybersecurity risk alongside other organizational risks (NIST, 2024). Similarly, ISACA’s COBIT 2019 framework distinguishes governance responsibilities, including evaluating, directing, and monitoring, from management activities performed by operational personnel, while recognizing risk and resource optimization as governance-level responsibilities rather than solely technical concerns (ISACA, 2019). ISO/IEC 27001:2022 also emphasizes management involvement by requiring organizations seeking certification to establish a documented information security management system with a defined scope, top-management commitment, and clearly assigned responsibilities, which align with the Governance Structure and Policy Formalization dimensions examined in this study. Collectively, these frameworks support the view that cybersecurity governance should be incorporated into organizational planning and resource-allocation processes, not treated solely as a downstream IT responsibility, providing the basis for the empirical examination undertaken in this study.

Sectoral Differences in Cybersecurity Governance

The integration of cybersecurity into organizational governance has progressed differently across sectors, with banking in the Philippines having a more established regulatory framework than the logistics industry. The Bangko Sentral ng Pilipinas (BSP) issued Circular No. 808 in 2013, requiring supervised financial institutions to incorporate information technology risk into their overall risk management frameworks and report their IT risk profiles as part of supervisory requirements (BSP, 2013). This was further strengthened by BSP Circular No. 982 in 2017, which emphasized appropriate governance structures, board-level accountability, and formal information security programs based on institutional complexity (BSP, 2017). These requirements place cybersecurity governance within the formal supervisory responsibilities of financial institutions. In comparison, 3PL and freight-forwarding firms in the Philippines do not have an equivalent sector-specific regulatory framework that directly assesses cybersecurity governance maturity. Although logistics providers are subject to regulations governing areas such as customs brokerage and land transportation, these requirements do not impose cybersecurity governance expectations comparable to those applied to BSP-supervised institutions. This gap is striking given that the Philippine National Cybersecurity Plan, issued by the Department of Information and Communications Technology (DICT), already designates transport and logistics among sectors considered critical information infrastructure, alongside banking, telecommunications, and power (DICT, 2017). The Cybercrime Prevention Act of 2012 (Republic Act No. 10175) provides a general legal framework by addressing unauthorized access, data interference, and other cybercrime offenses across industries, but it primarily focuses on criminal liability instead of establishing preventive cybersecurity governance requirements for organizations. The difference in regulatory treatment between banking and logistics therefore provides an important context for examining how cybersecurity governance is currently integrated into the planning and decision-making processes of Philippine 3PL firms and for considering appropriate voluntary governance benchmarks for the sector.

Third-Party Logistics, Digitalization, and Cyber Exposure

The absence of supervisory pressure does not mean 3PL firms carry less cyber exposure than banks. A 3PL firm's position inside its clients' supply chains creates its own exposure. Mid-market 3PL and freight-forwarding firms in the Philippines routinely hold client shipment manifests, warehouse-management credentials, and customs documentation, and a growing share integrate directly with enterprise clients' own enterprise resource planning or order-management systems through APIs to support real-time visibility and automated order processing. Each integration extends a client's attack surface into a vendor the client does not directly control, which is what NIST's supply chain risk management guidance treats as a defining feature of

modern cyber risk: an organization's security posture is only as strong as the weakest node in its supplier and logistics network (Boyens et al., 2015). Digitalization initiatives that 3PL firms undertake to win and retain enterprise clients, such as building an API gateway or adopting a client's electronic data interchange standard, raise the firm's cyber exposure without necessarily raising its governance capacity to manage that exposure. This gap between growing digital exposure and governance maturity is largely undocumented in the Philippine logistics literature, which has focused more on operational efficiency and cost than on governance.

Cybersecurity Governance Structure

Accountability is the foundation the other Govern categories build on, according to NIST CSF 2.0: who holds it, and whether it connects to enterprise risk management at all (NIST, 2024). Empirical work on how this plays out in practice, however, complicates the assumption that formal structure automatically produces substantive oversight. In a field study of corporate boards, Lowry, Vance, and Vance (2025) found that directors without cybersecurity expertise can perform the same oversight activities as expert directors, receiving briefings and sitting through updates, while the resulting oversight remains largely symbolic instead of substantive, and that nonexpert directors themselves rarely recognize the gap. Harel and Carmeli (2025) respond to this problem by proposing a sensemaking framework that asks boards to actively scan, interpret, and act on cybersecurity information across the threat lifecycle instead of passively receiving it, a distinction that maps closely onto this study's separation between receiving updates and actively participating in decisions. In the Philippine SME context specifically, Blancaflor et al. (2024) found that firms applying NIST and ISO frameworks derived clear benefits in incident response and stakeholder trust, but that framework adoption remained uneven and rarely reached formal, board-level ownership, a pattern this study's Governance Structure dimension was designed to measure directly.

Cyber risk management integration

This dimension asks a simple question: does cybersecurity risk sit inside the company's overall risk management process, or does IT handle it off to the side? NIST's supporting guidance for CSF 2.0 explicitly pairs the Govern function with enterprise risk management practice, treating cybersecurity risk as one input into a single organizational risk picture rather than a parallel process (NIST, 2024). For 3PL firms specifically, this integration carries added urgency because of third-party exposure: the World Economic Forum and Accenture's Global Cybersecurity Outlook 2024 found that roughly two in five organizations experiencing a major cybersecurity incident in 2023 traced it to a third-party vendor, and IBM's 2024 Cost of a Data Breach Report found that a majority of surveyed organizations had experienced a breach caused by a third party or supply-chain partner, with such breaches costing measurably more than the global average (International Business Machines Corporation, 2024; World Economic Forum & Accenture, 2024). A logistics firm's clients face exactly this exposure through the firm's own systems, which is what makes the escalation pathway from an identified cyber risk to a decision-maker that matters more for this dimension than the mere existence of a risk register.

Policy Formalization

SME cybersecurity research consistently finds the largest gap between practice and paper at the point where governance intent and risk awareness are supposed to become written, approved documents. ISO/IEC 27001:2022 makes a documented information security management system, with defined scope and top-management commitment, a certification requirement, but certification-oriented standards were built with large-enterprise compliance functions in mind (International Organization for Standardization, 2022). Garrone (2025), in a preprint currently under journal review, argues that this is a central reason formal compliance frameworks struggle to reach micro and small enterprises. In response, he proposes an awareness-first governance model — treating structured but lighter-weight practices, rather than full policy documentation, as the realistic entry point for firms operating under regimes such as the EU's NIS2 directive. That logic transfers directly to the mid-market Philippine 3PL context examined here: firms in this sector face no equivalent regulatory mandate to formalize policy at all, so whatever documentation exists reflects internal initiative rather than external requirement. Vendor and client contract clauses are the most telling indicator here — exactly where NIST's supply-chain guidance locates the weakest node in a client's own security posture (Boyens et al., 2015).

Resource Allocation

The question for this dimension is timing: is cybersecurity spending planned ahead of identified risks, or does it show up reactively once something has already gone wrong? The 2025 State of SMB Cybersecurity Report found that a majority of small and mid-sized businesses now rank cybersecurity as a top business priority, yet a comparable majority exceeded their cybersecurity budget in the same year, a pattern the report's

authors attribute to unplanned, incident-driven spending instead of deliberate risk-based planning (ConnectWise & Vanson Bourne, 2025). Separately, the IANS Research and Artico Search Security Budget Benchmark Report found that the share of revenue organizations dedicate to cybersecurity has risen steadily but still varies widely with no consistent link to a documented risk assessment (IANS Research & Artico Search, 2025). This gap between spending levels and risk-linkage is exactly what Gordon and Loeb's (2002) economic model of information security investment predicts will happen when budget decisions are made without a clear accounting of the risk being mitigated: firms invest, sometimes substantially, but without the analytic discipline that would let them show the investment is proportionate to exposure. This study's Resource Allocation dimension isolates that gap directly by separating tool investment from risk-linked budget justification.

Theoretical Perspectives on Cybersecurity Governance

Two organizational theories provide complementary perspectives for explaining differences in cybersecurity governance integration across firms: Agency Theory and Institutional Theory. Agency Theory, developed by Jensen and Meckling (1976), views the organization as a relationship between principals, such as owners or board members, and agents, such as managers and staff, whose interests and access to information may differ. Applied to cybersecurity, the theory suggests that when responsibility for cybersecurity rests primarily with an IT function or external provider with limited access to senior management, information about cyber risks may remain at the operational level. As a result, owners and senior executives may give limited attention to cybersecurity governance until a security incident or other event makes the risk more visible. Institutional Theory provides a complementary explanation through the concept of institutional isomorphism proposed by DiMaggio and Powell (1983), which suggests that organizations adopt similar structures and practices in response to coercive, mimetic, and normative pressures. Meyer and Rowan (1977) similarly argue that organizations may adopt formal structures to maintain legitimacy and respond to external expectations, even when these structures are not directly linked to operational efficiency. In the context of 3PL firms, this perspective suggests that cybersecurity governance may become more integrated when firms face external pressures, such as regulatory requirements or enterprise-client security assessments tied to API and system integrations. When such pressures reach senior management, they lead to formal, sustained governance practices. When cybersecurity stays an IT or contractor responsibility, integration stalls. Taken together, the two theories provide complementary explanations: Agency Theory helps explain why cybersecurity governance may remain underdeveloped in the absence of management visibility or accountability, while Institutional Theory helps explain how external pressures can encourage firms to formalize and integrate cybersecurity governance into organizational planning.

Across the literature reviewed, studies converge on one principle but differ by sector, firm size, and research method. International standards such as NIST CSF 2.0, COBIT 2019, and ISO/IEC 27001:2022, together with organizational theory, recognize cybersecurity governance as a planning-stage responsibility that should be integrated with financial and operational risk management (NIST, 2024; ISACA, 2019; International Organization for Standardization, 2022). However, this approach is more established in banking, where BSP regulations support board-level cybersecurity governance, than in mid-market 3PL and freight-forwarding firms, which carry substantial cyber exposure of their own but lack an equivalent regulatory framework (BSP, 2013, 2017; DICT, 2017). Existing studies also focus mainly on large enterprises or generic SMEs, leaving limited evidence on mid-market Philippine 3PL firms (Lowry, Vance, & Vance, 2025; Blancaflor et al., 2024; Garrone, 2025), a pattern Culot et al. (2022) trace to governance frameworks that are built for large enterprises and then scaled down rather than designed around smaller firms' own constraints. Methodologically, quantitative studies enable comparison but provide limited insight into why governance practices vary, while qualitative studies explain these differences but offer less basis for cross-firm comparison. Few studies combine both approaches within the same organizations. This study addresses both gaps at once, methodological and sectoral, through a convergent mixed-method multi-case design involving five mid-market Philippine 3PL firms, combining a 20-item extent-of-practice survey with key informant interviews and document review to assess cybersecurity governance across Governance Structure, Risk Management Integration, Policy Formalization, and Resource Allocation, and using the findings to develop a sector-specific framework for integrating cybersecurity governance into corporate planning.

Methodology

Research Design

This study used a convergent parallel mixed-method multi-case design (Creswell & Plano Clark, 2018). Quantitative survey data and qualitative interview and document data were collected concurrently across the five case firms, analyzed separately using methods appropriate to each strand, and merged at the interpretation

stage through a joint display. The multi-case component followed Yin's (2018) case study logic, treating each firm as a bounded case examined through survey responses, interviews, and documents, to allow within-case description and cross-case comparison. This design enabled the study to address two complementary questions using the same five firms: the extent of integration, measured comparably across 35 respondents, and the reasons for variation, explored through the perspectives of key informants.

Research Locale

The five participating firms operate primarily within the National Capital Region (NCR) and the adjoining CALABARZON and Central Luzon areas, which form a major corridor for third-party logistics and freight-forwarding activities due to their proximity to the Port of Manila, Manila International Container Terminal, Ninoy Aquino International Airport, and major industrial estates in Cavite, Laguna, and Bulacan. The main or head operating offices of the five case firms were distributed across Bulacan (1 firm), NCR (2 firms), Laguna (1 firm), and Cavite (1 firm), providing geographic variation within this key logistics corridor.

Research Participants

Research participants comprised two groups drawn from the same five case firms. The first group consisted of 35 structured-survey respondents occupying planning, executive management, finance, and information technology roles, selected based on their direct involvement in or exposure to cybersecurity-related planning and resource-allocation decisions. Respondent distribution across the five firms was uneven and loosely reflected firm size, with the larger firms (Firms C and D) contributing more respondents than the smaller firms (Firms A and E). The second group consisted of ten purposively selected key informants for the semi-structured interviews, with two representatives per firm, generally an owner or senior executive and the individual most directly involved in cybersecurity-related decisions, such as an IT head or operations executive. These key informants also served as the primary sources for the internal-document review.

Research Instrument

Three instruments were used to collect the quantitative and qualitative data examined in this study. The primary quantitative instrument was a structured 20-item survey adapted from the NIST Cybersecurity Framework (CSF) 2.0 Govern function (NIST, 2024) and selected COBIT 2019 governance and management objectives (ISACA, 2019). The survey comprised four five-item dimensions aligned with the study's four research sub-questions under Problem 1: Governance Structure, Risk Management Integration, Policy Formalization, and Resource Allocation. Each item was rated using a five-point Likert-type scale (1 = Strongly Disagree/Not Integrated to 5 = Strongly Agree/Fully Institutionalized), with item and dimension means interpreted as Not Integrated (1.00–1.79), Minimally Integrated (1.80–2.59), Moderately Integrated (2.60–3.39), Substantially Integrated (3.40–4.19), and Fully Institutionalized (4.20–5.00). The instrument demonstrated an overall good internal consistency (Cronbach's $\alpha = .83$). The qualitative strand employed a semi-structured key informant interview guide based on the same four dimensions to explore how and why the firms' survey-level results emerged, including triggering events, escalation of cybersecurity concerns to decision-makers, and identification of accountable owners. An internal document-review checklist further guided the collection and analysis of firm-provided artifacts, including information security policies, incident-response procedures, board or management meeting minutes, risk registers, and vendor or client contracts, which were used to corroborate and contextualize the survey and interview findings.

Data Gathering Procedure

Data collection was conducted in three concurrent stages consistent with the study's convergent parallel mixed-methods design. First, firm-level cooperation was secured from each of the five purposively selected firms through formal requests to firm owners or senior management, outlining the study's purpose, data-privacy safeguards, and anonymization procedures using Firms A–E. Second, the structured survey was administered to 35 eligible respondents either in person or through a secure online form, accompanied by an informed-consent form; completed responses were reviewed for completeness before encoding and analysis. Third, semi-structured interviews with ten key informants and the internal document review were conducted concurrently with the survey, with interviews audio-recorded with consent and transcribed verbatim, while firm-provided documents were collected and cross-checked against interview statements. Data collection for each firm was completed within the same general timeframe to maintain the study's cross-sectional, single-point-in-time design. All data were treated confidentially, with firm and individual identities replaced by the Firm A–E coding scheme and raw data securely stored and accessible only to the researcher.

Results and Discussions

Research Question 1: What is the extent of cybersecurity integration as a corporate planning function among mid-market Philippine logistics firms in terms of governance structure, risk management integration, policy formalization, and resource allocation?

Table 1. Extent of Cybersecurity Integration in terms of Governance Structure

Indicators	Mean	Verbal Description	Interpretation
1. A specific individual or role is formally designated as accountable for cybersecurity decisions.	2.80	Moderately Integrated	Accountability not formalized
2. The firm's board, owner, or top management receives regular updates on cybersecurity matters.	3.10	Moderately Integrated	Inconsistent leadership updates
3. Cybersecurity is a standing item in overall business planning meetings.	2.65	Moderately Integrated	Least consistently practiced
4. Roles and responsibilities for cybersecurity decision-making are clearly documented.	3.25	Moderately Integrated	Strongest documentation practice
5. Senior leadership actively participates in cybersecurity-related decisions.	2.90	Moderately Integrated	Limited active involvement
Dimension Mean	2.94	Moderately Integrated	Moderately integrated overall

Governance Structure came in second-lowest of the four dimensions in Problem 1. The two items measuring structural documentation, clearly documented roles and responsibilities ($M = 3.25$) and board or top-management updates ($M = 3.10$), scored highest, while the two items measuring active, habitual engagement, cybersecurity as a standing planning-meeting item ($M = 2.65$) and senior leadership's active participation in cybersecurity decisions ($M = 2.90$), scored lowest. The findings indicate that formal designation of responsibility was more prevalent than routine leadership participation in cybersecurity-related planning. This split mirrors Lowry, Vance, and Vance's (2025) finding that boards can perform the visible motions of oversight, receiving updates, checking a box, without that activity translating into substantive engagement. Agency theory would predict much the same outcome: information generated at the operational level does not automatically reach, or hold the attention of, the principals who set the planning agenda (Jensen & Meckling, 1976).

Table 2. Extent of Cybersecurity Integration in terms of Risk Management Integration

Indicators	Mean	Verbal Description	Interpretation
1. Cyber risk is recorded as a line item in the firm's overall risk register.	2.75	Moderately Integrated	Inconsistently recorded risk
2. Cyber risk is discussed alongside financial and operational risks during planning cycles.	3.05	Moderately Integrated	Moderately regular discussion
3. The firm has a documented process for escalating identified cyber risks to decision-makers.	2.60	Moderately Integrated	Weakest escalation process
4. Cyber risk assessments inform decisions on new client integrations or system changes.	3.30	Moderately Integrated	Strongest risk application
5. The firm reviews its cyber risk exposure on a regular (e.g., annual) basis.	3.10	Moderately Integrated	Fairly established review
Dimension Mean	2.96	Moderately Integrated	Moderately integrated overall

The overall score for Risk Management Integration, $M = 2.96$, was barely above Governance Structure's — but averaging the five items together hides a specific structural weakness rather than uniform mediocrity. Cyber risk assessments informing new client-integration or system-change decisions scored highest ($M = 3.30$), showing that firms do engage with cyber risk at the moment a concrete, consequential decision is on the table, exactly the kind of decision through which enterprise clients extend their own attack surface into a vendor's systems (Boyens et al., 2015). Yet the documented escalation process for identified cyber risks scored lowest of all five items in this dimension ($M = 2.60$), meaning the pathway through which risks

identified at the operational level reach decision-makers before a relevant decision is made therefore represents the weakest link in the governance process.

Table 3. Extent of Cybersecurity Integration in terms of Policy Formalization

Indicators	Mean	Verbal Description	Interpretation
1. The firm has a written, approved information security policy.	2.15	Minimally Integrated	Largely absent policy
2. The firm has a documented incident-response procedure for cybersecurity incidents.	2.35	Minimally Integrated	Underdeveloped incident procedures
3. Vendor or client contracts include specific cybersecurity or data-security clauses.	2.05	Minimally Integrated	Weakest overall item
4. Written cybersecurity policies are reviewed and updated on a defined schedule.	2.90	Moderately Integrated	Moderately consistent review
5. Employees receive documented guidance on their cybersecurity-related responsibilities.	3.05	Moderately Integrated	Strongest dimension item
Dimension Mean	2.50	Minimally Integrated	Weakest dimension overall

No dimension scored lower than Policy Formalization ($M = 2.50$, Minimally Integrated). Nearly every item in it landed at or near the Minimally Integrated band; only one broke the pattern. Vendor or client contracts including specific cybersecurity or data-security clauses scored lowest of all twenty survey items ($M = 2.05$), a finding that carries particular weight for 3PL firms because contractual clauses are the mechanism through which an enterprise client could otherwise hold its logistics vendor to a defined security standard, the exact weak-node problem NIST's supply-chain risk guidance describes (Boyens et al., 2015). Written, approved information security policy ($M = 2.15$) and documented incident-response procedures ($M = 2.35$) were similarly underdeveloped, in line with ISO/IEC 27001:2022's observation that formal documentation is the resource-intensive layer of an information security management system, one Garrone (2025) argues resource-constrained SMEs are structurally least equipped to complete even when their underlying practices are otherwise reasonable. Consistent with that account, the one item that scored appreciably higher, employees receiving documented guidance on their cybersecurity responsibilities ($M = 3.05$), suggests firms are communicating expectations informally to staff well before they get around to writing formal policy.

Table 4. Extent of Cybersecurity Integration in terms of Resource Allocation

Indicators	Mean	Verbal Description	Interpretation
1. The firm sets aside a specific line item in its budget for cybersecurity spending.	3.85	Substantially Integrated	Substantially integrated budgeting
2. Cybersecurity purchases are planned in advance rather than made only in response to an incident.	3.10	Moderately Integrated	Moderately proactive purchasing
3. The firm has invested in tools such as antivirus software, firewalls, or cloud backup services.	4.20	Fully Institutionalized	Highest-scoring item overall
4. Spending on cybersecurity is reviewed as part of the annual budgeting process.	4.05	Substantially Integrated	Substantially integrated review
5. Cybersecurity budget requests are linked to identified risks or planning priorities.	2.80	Moderately Integrated	Weakest risk linkage
Dimension Mean	3.60	Substantially Integrated	Substantially integrated overall

By a wide margin, Resource Allocation outscored every other dimension ($M = 3.60$, Substantially Integrated). Its strongest item — investment in tools such as antivirus software, firewalls, and cloud backup services ($M = 4.20$, Fully Institutionalized) — was also the single highest-scoring item in the entire twenty-item survey. Spending review as part of the annual budgeting process was similarly strong ($M = 4.05$). Yet the item asking whether cybersecurity budget requests are linked to identified risks or planning priorities scored

lowest within this dimension ($M = 2.80$), reproducing at the item level the exact pattern industry benchmarking data describes at the organizational level: spending has grown steadily, but the analytic discipline connecting that spending to a documented risk assessment lag behind it (ConnectWise & Vanson Bourne, 2025; IANS Research & Artico Search, 2025). This pattern is consistent with Gordon and Loeb's (2002) economic model of information security investment, which suggests that budgeting decisions should be informed by the relationship between identified risks and security investments. It also directly informs this study's Resource-Alignment layer, which proposes requiring every new budget request to reference a specific risk already documented in the firm's risk register.

Table 5. Summary of Extent of Cybersecurity Integration for the Five Firms

Firm	Governance Structure	Risk Mgmt. Integration	Policy Formalization	Resource Allocation	Overall Mean	Verbal Description	Interpretation
1. A	2.05	2.15	1.70	2.90	2.20	Minimally Integrated	Lowest overall score
2. E	2.10	2.25	1.85	3.20	2.35	Minimally Integrated	Second-lowest overall score
3. B	2.80	2.95	2.45	3.72	2.98	Moderately Integrated	Mid-tier, transitional profile
4. D	3.70	3.60	3.15	4.05	3.63	Substantially Integrated	Second-highest overall score
5. C	4.05	3.85	3.35	4.15	3.85	Substantially Integrated	Highest overall score
Mean	2.94	2.96	2.50	3.60	3.00	Moderately Integrated	Moderately integrated overall

The dimension-by-firm breakdown in Table 5 makes visible a pattern that holds at every firm regardless of overall tier: Resource Allocation is each firm's highest-scoring dimension and Policy Formalization its lowest, from Firm A's minimally integrated profile (2.90 versus 1.70) through Firm C's substantially integrated one (4.15 versus 3.35). That consistency suggests the two dimensions are shaped by different mechanisms. Resource Allocation's uniformly higher scores, even among low-tier firms, fit the mimetic and normative isomorphism institutional theory describes: buying recognizable tools such as antivirus software or cloud backup is a visible, relatively low-cost way for a firm to signal legitimacy to clients and peers regardless of whether a deeper governance structure exists behind the purchase (DiMaggio & Powell, 1983; Meyer & Rowan, 1977). Policy Formalization's uniformly lower scores, by contrast, point to a genuine capacity constraint: writing and approving formal documentation requires a principal-level mandate and sustained administrative effort that Garrone (2025) argues resource-constrained firms are least equipped to supply, which is why even Firms C and D, otherwise Substantially Integrated, had not closed this particular gap.

Research Question 2: How does the extent of cybersecurity–corporate planning integration vary across the five case firms in relation to firm size, years in operation, and the presence of enterprise API/system integrations with clients?

Table 6. Cybersecurity–Corporate Planning Integration by Firm Size, Years in Operation, and Client API Integration Level

Tier	Firms	Firm Size	Years in Operation	API Integration Level	Mean	Verbal Description	Interpretation
1. Tier 1	A, E	Small (< 100 employees)	0–9 years	None	2.28	Minimally Integrated	Limited planning bandwidth
2. Tier 2	B	Medium (100–249 employees)	10–14 years	Limited	2.98	Moderately Integrated	Uneven, transitional integration
3. Tier 3	C, D	Large (250+ employees)	15+ years	Extensive	3.74	Substantially Integrated	Scale enables formal oversight

Table 6 shows overall integration scores across the three firm-level variables examined under Problem 2: firm size, years in operation, and API integration level. In these five firms, the three variables are fully collinear, forming the same three-tier grouping: Firms A and E are the smallest, newest, and least API-integrated; Firm B is medium-sized, mid-tenure, and has limited API integration; and Firms C and D are the largest, longest-established, and most extensively integrated. Thus, all three variables show the same progression from Minimally Integrated ($M = 2.28$) to Moderately Integrated ($M = 2.98$) and Substantially Integrated ($M = 3.74$), rather than three independent effects.

This collinearity is itself a finding and limits the ability to identify which variable drives integration within the five purposively selected firms. A larger and more diverse sample is therefore needed to isolate their individual effects. Nevertheless, each variable provides a plausible explanation consistent with Institutional Theory and its concept of isomorphic pressure (DiMaggio & Powell, 1983). Larger firms may have greater capacity to establish specialist governance functions; longer-established firms have had more exposure to client compliance reviews and vendor security assessments; and greater API integration increases exposure to enterprise-client security requirements and supply-chain cyber risks (Jeyaraj & Zadeh, 2020; Boyens et al., 2015). These pressures help explain why Firms C and D developed stronger governance practices. Firm B further shows that greater API exposure does not automatically translate into stronger governance integration; exposure creates pressure, but integration depends on a governance structure capable of converting that pressure into organizational practice.

Table 7. Overall Integration Score by Firm Characteristics

Firm	Employees	Years	API Integration	Board/Oversight	Overall Mean	Tier
1. A	45	6	None	None	2.20	Minimally Integrated
2. E	28	4	None	None	2.35	Minimally Integrated
3. B	120	12	Limited	Informal	2.98	Moderately Integrated
4. D	260	15	Extensive	Formal	3.63	Substantially Integrated
5. C	310	18	Extensive	Formal (advisory)	3.85	Substantially Integrated

Table 7 assembles all four firm-level variables side by side and shows that no single characteristic sorts the five firms into their eventual tier as cleanly as the combination of extensive client API integration and formal board or advisory-level oversight. Firms C and D share both characteristics and are the only two firms classified Substantially Integrated (3.85 and 3.63). Firm B holds a client API integration but only informal oversight, and lands at Moderately Integrated (2.98); Firms A and E hold neither characteristic and land at Minimally Integrated (2.20 and 2.35). This is the empirical basis for the study's central claim under Problem 2 and Problem 5: firm size and years in operation correlate with integration but do not explain it on their own, while the joint presence of client-driven exposure and a governance body positioned to receive it does. That combination is also where agency theory and institutional theory meet in this dataset, exposure alone supplies the information (or, per agency theory, fails to reach the principal without a pathway; Jensen & Meckling, 1976), while a receiving governance body supplies the mechanism institutional theory identifies as necessary to convert external pressure into durable structural change (DiMaggio & Powell, 1983).

Research Question 3: What factors explain differences in cybersecurity governance integration into each case firm's corporate planning process?

Reflexive thematic analysis of the interview and document data surfaced three themes that explain the dimension-level and firm-level patterns above better than any single structural variable does on its own. The first and most consistent theme was that a triggering event got converted into a standing planning practice in Firm C and Firm D, but not in Firms A, B, or E. In Firm C, an informant described a client-mandated vendor security review as the moment cybersecurity moved from an IT conversation to a board-level agenda item; prompted by the enterprise client's own compliance requirements, the review has since become a recurring, calendared part of the firm's annual planning cycle rather than a one-time exercise. In Firm D, the driver sat closer to the firm's core service: pharmaceutical and cold-chain clients' regulatory and data-integrity expectations made cyber and data risk inseparable from the operational compliance the firm already reported to its board, so a risk committee originally formed for cold-chain compliance took on cybersecurity oversight as a natural extension. In both firms, an external actor — a client or a client's compliance requirement — supplied the pressure, while an existing or newly formed governance body supplied the mechanism that made the response stick, the coercive-isomorphism pathway institutional theory describes (DiMaggio & Powell, 1983).

The second theme was the mirror image of the first: cybersecurity stayed an unescalated IT-contractor matter in Firms A, B, and E. Informants at these firms did not describe cybersecurity as ignored. Each could point to a past incident, a phishing attempt, a vendor's ransomware scares, a client asking about data handling, but in every case the incident got resolved at the technical level, by an internal IT staff member or an outsourced provider, and never became a standing planning input. Firm B stood out here: despite holding a client API integration, the firm's response to a phishing incident several years earlier amounted to handing it to IT to fix, never treating it as an occasion for board-level review. Agency theory has an explanation for that: risk information available to an operational agent does not automatically reach the principals who set the planning agenda (Jensen & Meckling, 1976), and it explains why Firm B's API integration alone did not push it into the

Substantially Integrated tier: exposure without an escalation pathway did not translate into governance change.

The third theme was where accountability sat. In Firms C and D, informants could name a specific individual, in each case a senior finance or operations executive rather than an IT manager, whom others in the firm understood to be the person now raising cybersecurity in planning discussions. In Firms A, B, and E, no informant could name such a person; responsibility was described as diffuse, or as resting with whoever happened to handle a given incident. This theme largely tracked the first two, a named owner tended to show up where a triggering event had already been escalated through a governance body — it did not appear to drive the pattern on its own — but it still mattered for framework development: naming an accountable owner is a concrete step lower-scoring firms could take even before a triggering event occurs.

Research Question 4: What patterns emerge from the integration of quantitative and qualitative findings across the five case firms?

Table 8. Joint Display of Quantitative Tier and Qualitative Themes by Firm

Firm	Quantitative Tier	Dominant Qualitative Theme(s)	Convergence / Nuance
A	Minimally Integrated	Cybersecurity as unescalated IT-contractor matter; no named owner	Convergent - qualitative account explains why score is lowest
E	Minimally Integrated	Same pattern as A; newest, smallest firm; no board to escalate to	Convergent - structural absence of any governance body reinforces score
B	Moderately Integrated	API exposure present but incident not escalated; no named owner	Convergent, with nuance - exposure without escalation explains a moderate rather than low or high score
D	Substantially Integrated	Triggering event (client compliance pressure) absorbed by existing risk committee; named owner	Convergent - qualitative account explains high score via institutional/compliance pathway
C	Substantially Integrated (highest)	Triggering event (client vendor review) converted to standing board practice; named owner	Convergent - qualitative account explains highest score via client-driven coercive pressure

The two data strands line up closely: in every firm, the qualitative themes informants described match and help explain that firm's quantitative tier. The strands corroborate each other; they do not pull in different directions. The clearest payoff from the joint display shows up in Firm B. Its quantitative score alone, a moderate result sitting between two clear tiers, could be read several ways, but the qualitative account settles it: Firm B was not partially integrated in some averaged sense, it was specifically exposed without an escalation pathway, a distinct condition rather than a midpoint on a continuum. That distinction shaped the second layer of the proposed framework. The broader pattern behind it, coercive pressure from a client converting into durable structural change only where a governance body exists to receive it, matches both institutional theory's empirical record in cybersecurity specifically and the public-policy literature on organizational triggers more generally. Jeyaraj and Zadeh (2020) found coercive pressure had the strongest near-term effect on cybersecurity responses in their study of 87 organizations, and Birkland (1998) found, in a different domain entirely, that a sudden, attention-grabbing event produces lasting change only when an existing structure is positioned to absorb and act on it.

Research Question 5: What model can be developed from the integrated findings to embed cybersecurity governance into corporate planning among mid-market Philippine logistics firms?

The findings from Problem 1 through Problem 4 point to four conditions that, present together, set the two Substantially Integrated firms apart from the three Minimally or Moderately Integrated firms. A governing body needs visibility into cyber risk. A checkpoint needs to weigh cyber risk before a planning decision, whether a capital expenditure, a new client onboarding, or a new system/API integration, gets approved. Cyber risk needs a place in the firm's broader risk-management vocabulary instead of sitting apart as an IT-only concern. And budget allocation needs to follow identified risk priorities instead of defaulting to familiar, easy-to-approve purchases. Table below summarizes the four-layer model built from these conditions.

Table 9. Proposed Four-Layer Model for Embedding Cybersecurity Governance into Corporate Planning

Layer	Core Question It Answers	Derived From	Practical Mechanism
1. Governance	Who is accountable, and does that person or body have visibility into cyber risk?	Research Question 1 Governance Structure dimension (named-accountability and leadership-participation items); Research Question 3 named-owner theme; Research Question 2 oversight-body presence	Name a specific executive-level owner; give a board, advisory board, or existing risk/compliance committee standing visibility into cyber risk, even before a formal CISO role exists
2. Planning-Gate	Is cyber risk reviewed before a relevant plan, contract, or system change is approved, or only after?	Research Question 1 Risk Management Integration items on escalation and on assessments informing new-integration decisions; Research Question 3 triggering-event-to-standing-practice theme; Research Question 4 Firm B's exposure-without-escalation pattern	Insert a cybersecurity checkpoint into approval workflows already used for capital expenditure, new client onboarding, and new system/API integrations, rather than creating a parallel process
3. Risk-Integration	Does cyber risk appear in the same risk vocabulary and register the firm already uses for other enterprise risks?	Research Question 1 Risk Management Integration dimension overall, particularly the risk-register and regular-review items; agency-theoretic information asymmetry	Add cyber risk as a standing line item in whatever risk register, insurance review, or client-contract risk clause process the firm already maintains, rather than a separate IT list
4. Resource-Alignment	Is what the firm spends on cybersecurity tied to what the first three layers identify as priorities?	Research Question 1 Resource Allocation dimension, particularly the gap between tool investment and risk-linked budget requests	Require that new cybersecurity budget requests reference an identified item from the Layer 3 risk register, closing the gap between generous ad hoc spending and thin formal risk identification

Policy Formalization, the weakest of the four survey dimensions under Problem 1, does not map onto a single layer above; adding a fifth, standalone layer for it did not fit the findings as well as treating it as a documentation requirement running through all four. Governance needs a written designation of who is accountable. Planning-Gate needs a written checkpoint procedure. Risk-Integration needs a written risk-register entry. Resource-Alignment needs a written justification linking spend to risk. Seen this way, Policy Formalization's low score at every firm, including C and D, means that even the two most-integrated firms had not finished writing down practices they were otherwise already following. That looks like an implementation gap, not a missing fifth layer.

The model is layered, not strictly sequential. Firms C and D did not build governance, then a planning gate, then risk integration, then resource alignment in that order; each layer reinforced the others once a triggering event and a receiving governance body were both in place. Its practical value comes from using mechanisms these firms already had, an existing board or advisory committee, an approval workflow, a risk register or insurance review, a budget cycle, instead of prescribing new specialized structures such as a dedicated CISO office or a formal enterprise risk management function, which informants across all five cases suggested would be hard to staff or justify on cost grounds. In that sense the framework translates the Govern-function and COBIT governance-objective logic reviewed earlier into a form sized for mid-market Philippine logistics firms, not a scaled-down version of a large-enterprise governance program. It also responds to the gap Culot et al. (2022) identified earlier: a framework built outward from what mid-market firms can actually staff and afford, rather than a large-enterprise governance program scaled down to fit.

Ethical Considerations

This study followed standard ethical protocols for research involving human participants and organizational data and was reviewed and approved by the University of Luzon's Graduate School Research Ethics Committee before data collection. Firm-level cooperation was secured through formal requests to owners or senior management, followed by informed consent from all 35 survey respondents and 10 key informants. Participation was voluntary, with participants free to decline questions or withdraw. No deception was used, and interviews were audio-recorded and transcribed only with explicit consent. Confidentiality was given particular attention because the study examined firms' cybersecurity governance practices and past security incidents, which could create reputational or competitive risks if disclosed. Firms were therefore coded as Firms A–E from the point of data collection, and identifying information was not retained with the analysis.

files. Raw data, including recordings, transcripts, policies, risk registers, and meeting minutes, were accessible only to the researcher and stored on encrypted, password-protected systems in accordance with the Data Privacy Act of 2012 (Republic Act No. 10173).

Conclusion

This study concluded that cybersecurity governance is integrated into corporate planning to varying degrees among mid-market Philippine third-party logistics (3PL) and freight-forwarding firms. The findings suggest that integration is influenced less by firm size or years in operation than by the combination of client-facing system integration and the presence of a governance structure capable of translating cybersecurity risks into organizational decisions. The more integrated firms had folded cybersecurity into planning, risk management, policy development, and resource decisions; the less integrated ones had simply left it with IT or an outsourced provider. The study contributes to knowledge by extending the concept of cybersecurity governance as a planning-stage responsibility beyond highly regulated sectors such as banking and applying it to the less-studied context of mid-market logistics firms. It also shows what mixing quantitative and qualitative evidence can do: measure how much integration exists, and explain why. In practice, the study proposes a four-layer framework—Governance, Planning-Gate, Risk-Integration, and Resource-Alignment—to help mid-market 3PL firms strengthen accountability, integrate cyber risk into corporate planning, and align cybersecurity investments with organizational risks. Given the purposive selection of five firms, all operating within the NCR–CALABARZON–Central Luzon corridor, the findings support analytic rather than statistical generalization and may not extend to 3PL firms in other Philippine regions without further testing. Future research should test the proposed framework using larger and more diverse samples, examine firm size, organizational age, and system integration as independent factors, and use longitudinal or comparative designs to assess how cybersecurity governance develops over time. Whether it travels beyond logistics and freight-forwarding is still an open question.

Recommendations

For mid-market 3PL and freight-forwarding firms, particularly those where cybersecurity remains primarily an IT responsibility, leadership should designate a clear executive owner for cyber-risk information. That owner needs a seat in existing planning, risk, and budgeting processes — not a parallel one. Firms should fold cybersecurity into the risk registers, insurance reviews, and client or contract requirements they already maintain instead of creating parallel processes, and should align security spending with documented risk priorities. Industry associations and trade bodies may develop a voluntary sector-specific cybersecurity governance benchmark based on the proposed framework, which would let firms demonstrate governance maturity to enterprise clients without adding a new regulatory burden; policymakers, for their part, could build on that same voluntary logic, developing sector-specific guidance for logistics and freight-forwarding firms through incentive-based approaches rather than mandates, while still recognizing the sector's role in national critical infrastructure. Future research should validate the framework with larger, more diverse samples, then track its durability longitudinally, examining how external triggers such as client requirements or security incidents lead to sustained governance change, and whether replication in other digitally exposed sectors shows the framework is transferable or requires sector-specific adaptation.

References

- Bangko Sentral ng Pilipinas. (2013). Guidelines on information technology risk management for all banks and other BSP supervised institutions (Circular No. 808, s. 2013). <https://www.scribd.com/document/467307020/BSP-Circular-808-s-2013-searchable>
- Bangko Sentral ng Pilipinas. (2017). Enhanced guidelines on information security management (Circular No. 982, s. 2017). <https://lpr.adb.org/sites/default/files/2024-05/philippines-c982.pdf>
- Birkland, T. A. (1998). Focusing events, mobilization, and agenda setting. *Journal of Public Policy*, 18(1), 53–74. <https://doi.org/10.1017/S0143814X98000038>
- Blancaflor, E., Pasco, J. A., Tamargo, J., Jonson, J. A., & Doydoy, J. D. (2024). Comparative analysis and application of cybersecurity framework to Philippine small and medium enterprises (SMEs). In *Proceedings of the 2024 9th International Conference on Intelligent Information Technology* (pp. 1–7). Association for Computing Machinery. <https://doi.org/10.1145/3654522.3654565>
- Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2015). Supply chain risk management practices for federal information systems and organizations (NIST Special Publication 800-161). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-161>

- ConnectWise, & Vanson Bourne. (2025). 2025 state of SMB cybersecurity report. ConnectWise. <https://www.connectwise.com/globalassets/media/asset-docs/executive-briefs/the-state-of-smb-cybersecurity-in-2025.pdf>
- Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications. <https://uk.sagepub.com/en-gb/asi/designing-and-conducting-mixed-methods-research-international-student-edition/book258100>
- Department of Information and Communications Technology. (2017). National cybersecurity plan 2022. Republic of the Philippines. <https://database.cyberpolicyportal.org/api/files/1669373681028wbvn87gdwah.pdf>
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- El-Hajj, M., & Mirza, Z. A. (2024). Protecting small and medium enterprises: A specialized cybersecurity risk assessment framework and tool. *Electronics*, 13(19), Article 3910. <https://doi.org/10.3390/electronics13193910>
- Garrone, R. (2025). Proportionate cybersecurity for micro-SMEs: A governance design model under NIS2 (arXiv:2511.02898). arXiv. <https://arxiv.org/abs/2511.02898>
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457. <https://doi.org/10.1145/581271.581274>
- Harel, Y., & Carmeli, A. (2025). A strategic cybersecurity oversight framework: A board's imperative. *Journal of Cybersecurity*, 11(1), Article tyaf021. <https://doi.org/10.1093/cybsec/tyaf021>
- IANIS Research, & Artico Search. (2025). 2025 security budget benchmark report. IANS Research. <https://www.iansresearch.com/resources/press-releases/detail/ians-research-and-artico-search-release-security-budget-benchmark-report>
- International Business Machines Corporation. (2024). Cost of a data breach report 2024. IBM Security. <https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>
- International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC 27001:2022). <https://www.iso.org/standard/82875.html>
- ISACA. (2019). COBIT 2019 framework: Governance and management objectives. <https://www.isaca.org/store2/product/WCB19FGM>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce*, 30(4), 361–380. <https://doi.org/10.1080/10919392.2020.1776033>
- Lowry, M. R., Vance, A., & Vance, M. D. (2026). Inexpert supervision: Field evidence on boards' oversight of cybersecurity. *Management Science*, 72(2), 783–804. <https://doi.org/10.1287/mnsc.2023.04147>
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
- National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Republic Act No. 10173, Data Privacy Act of 2012. (2012). Congress of the Philippines. <https://lawyerly.ph/laws/view/lc44d>
- Republic Act No. 10175, Cybercrime Prevention Act of 2012. (2012). Congress of the Philippines. <https://ldr.senate.gov.ph/legislative-issuance/republic-act-no-10175>
- von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- World Economic Forum, & Accenture. (2024). Global cybersecurity outlook 2024. World Economic Forum. <https://www.weforum.org/publications/global-cybersecurity-outlook-2024/>
- Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.