Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 2, 441-459
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i2.310

Evaluating Cybersecurity Investment Strategies in a Medium-Sized Enterprise: A Case Study of a Growing POS Service Provider in Indonesia

Ryan Adhi Nugraha[1*]
Universitas Indonesia, Depok, Indonesia

Muhammad Hafizhuddin Hilman[2]
Universitas Indonesia, Depok, Indonesia

Setiadi Yazid[3]
Universitas Indonesia, Depok, Indonesia

Eko Yon Handri[4]
Universitas Indonesia, Depok, Indonesia

***Corresponding author:**
Ryan Adhi Nugraha, Universitas Indonesia, Indonesia. ✉ryan.adhi@ui.ac.id

Article Info:

Article history:
Received: March 27, 2026
Revised: May 20, 2026
Accepted: May 23, 2026

Keywords:
cybersecurity strategy; medium-sized enterprise; proactive security; reactive security; SaaS POS.

Abstract

Background: As medium-sized businesses use third-party integrations in SaaS-based POS systems, cybersecurity concerns expand the potential attack surface. Many of these organizations engage in reactive cybersecurity, waiting until incidents occur rather than implementing preventive measures. In the face of increasingly complex organizational architectures, it is imperative to reevaluate whether these reactive approaches remain adequate in guaranteeing operational continuity and data security.
Objective: This research aims to examine whether a reactive cybersecurity approach may still suffice for a medium-sized company expanding its operations in Indonesia and operating on a SaaS POS platform.
Method: The study uses a qualitative single-case study design. Data were collected through semi-structured interviews with business and engineering stakeholders, triangulated with supporting organizational documents. Data were analyzed using rubric-based qualitative coding and mapped against a literature-derived reactive–proactive cybersecurity posture rubric regarding incident response, budget allocation, and layered security infrastructure.
Results: The findings suggest that daily operational readiness is limited by symptom-driven detection systems, periodic and manual monitoring practices, and response schedules dependent on unstructured coordination and follow-ups. While baseline preventive controls exist, many program-level capabilities remain nascent from centralized telemetry and alerting to consistent incident workflows with remediation tracking indicating an imbalance between reactive practices and a systematic, continuous cadence of security assurance.
Conclusion: The findings indicate that a reactive cybersecurity posture is inadequate for the case organization. The company exhibits symptom-driven detection, informal incident coordination, and episodic budget allocation. A gradual transition toward proactive practices is recommended, prioritizing centralized observability, and structured incident workflows.

To cite this article: Nugraha, R. A., Hilman, M. H., Yazid, S., & Handri, E. Y. (2026). Evaluating Cybersecurity Investment Strategies in a Medium-Sized Enterprise: A Case Study of a Growing POS Service Provider in Indonesia. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(2), 441-459. https://doi.org/10.59261/jequi.v8i2.310

INTRODUCTION

Increasingly, organizations must carefully consider potential digital threats that have become more common and costly, especially due to the effects of operational downtime, recovery expenses, and possible cascading consequences that extend beyond simply addressing the technical aspects (Romanosky, 2016; Saad, 2026). Operational excellence in attack surface management, observability (centralized monitoring and analysis), and vulnerability and incident response has been shown to dramatically affect the security posture of cloud services, especially when it comes to SaaS platforms with public-facing endpoints and third-party integrations (Naseer et al., 2023) Moreover, evidence from major breach cases illustrates that escalation often results in reputational damage and longer recovery times when weaknesses exist throughout an incident's lifecycle (Khan et al., 2023).

Cybersecurity posture is usually framed in a reactive–proactive dichotomy. Reactive postures act after the fact, typically focusing on rapid service restoration rather than eliminating root causes or enabling continuous improvement (Furnell et al., 2020; Liu & Babar, 2026). Proactive postures emphasize preventative and detective controls facilitated by defined workflows, continuous monitoring, and systematic improvement processes to reduce both the probability and impact of breaches, as shown by Naseer et al. (2023). In reality, organizations should operate under a unified posture of controls spanning detection, containment, recovery, and learning (Zhong et al., 2024). Where systems scale and integrations increase, exposure and response requirements can outstrip capacity; propagation of third-party risk (Oriola et al., 2021; Ruohonen et al., 2025) is therefore governed by budget constraints and policy landscapes that determine which capabilities can be funded (Magdy & Crispm, 2026; Pech & Vrchota, 2020).

The same can be said for medium-sized enterprises (MSEs), where these challenges are even more pronounced. MSEs generally operate under tighter budgets and with fewer specialist resources compared to their larger counterparts, yet they frequently run services with very high transaction volumes and availability expectations, making security and resilience operationally critical (Gao et al., 2023). However, empirical evidence specifically regarding MSE cybersecurity, as well as other contributing factors, is still limited relative to larger firms; moreover, risks for MSEs may exceed their ability to fully implement preventative controls (Romanosky, 2016; Saad, 2026). This study classifies enterprise size based on number of employees and annual revenue using frequently cited quantitative measures (Berisha & Pula, 2015; Olipp et al., 2026), as shown in Table 1.

Table 1. Enterprise Classification

Classification	Employee Count	Annual Revenue (USD)
Micro Enterprise	< 10	< 100,000
Small Enterprise	10–49	100,000–3,000,000
Medium Enterprise	50–249	3,000,000–15,000,000
Large Enterprise	≥ 250	> 15,000,000

source: research data

This paper bridges the gap identified above and undertakes a qualitative single-case study of an expanding SaaS provider in Indonesia's POS space. Its customer base comprises retail and restaurant merchants that rely on integration patterns within POS ecosystems (where partner-led payment experiences occur, along with the compliance expectations that accompany them). The organization in the case has a history of a recent security incident involving an API-facing service, which highlighted the limitations of relying solely on reactive incident handling and prompted the use of an objective assessment approach as a means of evolving its cyber security posture (Furnell et al., 2020; Liu & Babar, 2026).

The research assesses security posture across three capability domains: incident response practices, budget allocation patterns, and the maturity of security infrastructure. The article adopts commonly used definitions of reactive and anticipatory responses but extends them to include both reactive (preventive or compensatory) and proactive mechanisms that policymakers may leverage to catalyze change in resource-constrained contexts, such as risk transfer

instruments (Wang et al., 2024). This paper aims to find out: (1) How does the organization's cybersecurity posture compare against reactive, mixed, and proactive characteristics across the three capability domains? (2) What gaps and staged investment priorities offer the best cost-effectiveness in improving day-to-day operational readiness within reasonable constraints?

This work provides (1) an ordered mapping strategy for linking benchmarks to evidence when assessing reactive versus proactive posture in an MSE SaaS environment with integrations, (2) a clear posture rubric aimed at improving replicability and reducing interpretive ambiguity, and (3) an evidence-based gap profile supporting the general features of a pragmatic transition path. Accordingly, as a qualitative single-case study, the findings are intended to be transferable in terms of assessment logic and practical insights rather than causal generalization.

METHOD

This study employed a qualitative case study design to determine whether a primarily reactive cybersecurity posture remained adequate for an expanding medium-sized enterprise (MSE) in Indonesia's point-of-sale (POS) SaaS vertical. Qualitative single-case analysis allowed for in-depth exploration of the areas needed to assess posture adequacy within a single unit and in an actual operational environment, since pressures from growth, real resource constraints, and external and third-party integration dependencies all existed. The case organization, anonymized here as "Company X," was chosen because it operated under integration dependencies common to POS ecosystems and had experienced an incident in which a reporting page dependent on a third-party API encountered an issue that could increase operational risk and response demands (Li & Xu, 2021; Wang & Xu, 2026).

Case Context and Classification

The unit of analysis was organizational cybersecurity posture, operationalized as observable, practice-based security capabilities under three dimensions: (i) incident response and épisteme, (ii) resource allocation and management, and (iii) defense infrastructure and depth. In this context, practice is defined as observable patterns of implemented practices and technical routines (monitoring and alerting frameworks, incident workflow artifacts, and control checks at regular intervals to assess compliance with a stated state or policy claim) rather than stated intentions or policy claims. The analysis marshals centralized logging, monitoring, and alerting capabilities as discriminating operational signals of posture maturity to anchor "observability" in concrete evidence (Younus & Alanezi, 2023). Instead of ad hoc narratives, the study focuses on security funding and prioritization on traceable program decisions and governance-oriented performance measurement practice indicators (Herath et al., 2022).

A widely used method to classify companies as MSEs is based on the number of employees and financial size (annual revenue). Many enterprise classification schemes apply firm-size measures based on employee count and annual revenues (Herath et al., 2022 López-Ortega et al., 2016), and common practice also employs employee-based size groupings, although thresholds vary among schemes (Berisha & Pula, 2015; Olipp et al., 2026). The organization and internal identifiers were anonymized.

Data Sources and Collection

Between January and December 2025, we conducted face-to-face semi-structured interviews to gather primary data. Sessions were audio-recorded, transcribed, and lasted approximately 30–45 minutes. Interviews were conducted in one-on-one or small focus-group discussion (FGD) formats. Qualitative case reporting, in seeking to improve transparency and reduce potential interpretive ambiguity, maintains an audit trail between interview questions, coded excerpts, and analytical claims through an evidence log and systematic reporting procedures (Alpi & Evans, 2019; Belkina et al., 2025).

To provide a technical and business overview, four different parties were interviewed: Project Manager; Lead Developer; Business Development Director; and Sales Team Lead. The approaches to Gemba, thus far, tend to be fairly abstract and opinionated rather than derived from specific and tangible accounts of operational practice in recent memory. Past these attendees,

participants listed common incidents and shared examples of recent cases that detail how detection was triggered, what monitoring or log evidence was reviewed, who coordinated containment, remediation steps taken afterward, post-incident outputs put into place, and how security work was prioritized and funded. The probes queried whether those activities were either routine or on demand and whether the controls were centralized and automated or local and manual, including whether alerting and analysis were backed by centralized monitoring practices (Younus & Alanezi, 2023).

Benchmark Instrument and Posture Rubric (reactive vs proactive)

Subjectivity was minimized and replication supported by identifying and using posture indicators from the literature that operationalize reactive and proactive cybersecurity in terms of observable patterns in practice (Shaikh & Siponen, 2023). The indicator set served as a non-prescriptive framework for structuring domain comparisons in the Results section and maintaining consistent benchmark-to-evidence mapping across domains. The aim is to bolster operational interpretability, and this emphasis concentrates on signals that run directly through daily operations, such as centralized monitoring, alerting, and analysis (Younus & Alanezi, 2023), or implementing governance practices across the program level that integrate security work into cyclical stages of repeatable oversight and executive review practices (Herath et al., 2022).

A reactive posture was indicated where practice patterns were mainly driven by the detection of or response to symptoms, periodic and manual monitoring and verification, informal coordination for response planning, and sharing of information in post-incident learning contexts, with funding effectively decided on a case-by-case basis rather than guided by a sustained trajectory of investment (Furnell et al., 2020; Liu & Babar, 2026). Alternatively, results suggested a largely preemptive stance when guided by continuous telemetry, centralized monitoring, and automation of practice patterns structured through incident workflows with defined roles, layered defenses solidified through sustained assurance loops, and repeatable operational routines (Naseer et al., 2023). The rubric also considers a portfolio view of controls and governance as supporting evidence in the infrastructure and control domain when investment choices are made through structured prioritization underpinned by governance-facing measurement, rather than ad hoc selection (Sawik & Sawik, 2022). In some areas, the benchmark acknowledges that organizational security investment behavior and timing of preventive controls are influenced by external policy environments that can shape budgeting and prioritization (Wang et al., 2024), including under explicit budgetary constraints by impacting what investment paths remain feasible (be they toward prevention or response) (Gao et al., 2023).

We assessed each criterion through pairs of reactive and proactive indicators found in the literature. Evidence was tabulated only when it corresponded to real-world practice; statements without corroborating artifacts or traces of engineering activity were recorded as not evidenced and did not lend support to either posture. Criteria were classified as predominantly reactive, predominantly proactive, or mixed depending on which sets of indicators were evidenced and whether proactive components were routine. Domain summaries consolidated these labels. Claims that participants made related to measurement were only considered as evidence (to minimize over-interpretation) if they described repeatable metrics or review practices used to inform decisions, and were not included if they referenced measures in aspirational terms (Carvalho et al., 2025; Jardine, 2018).

The five-year outlook, therefore, is more a data-informed trajectory than a prediction. It presupposes a baseline scenario where both constraints and operating patterns including resource limitations and dependency-driven exposure are similar. Thus, the outlook provides continuity where it aligns with current trends, gradual improvement where low-hanging fruit is conceivable without formal commitments, and no claimed major change when signals at the program level are not identifiable. Commitment signals were construed as supporting evidence such as named ownership, timelines, durable funding, or a cadence of governance practices that underpin capability building beyond an incident-driven feedback loop (Gao et al., 2023).

Evidence Mapping, Validity, and Ethics

The method mapped evidence to benchmarks and was replicable. We checked the completeness of interview transcripts, categorized them into three cost domains, and correlated excerpts illustrating company X practices with paired reactive and proactive indicators to classify each criterion as primarily reactive, predominantly proactive, or mixed. We cross-verified findings from different roles by comparing technical and business accounts before consolidating them into comparison tables across benchmark indicators, observed practices, and resulting judgments. These focus areas of developing traceable evidence chains and clear mapping logic are also widely recommended for improving case study reporting quality, for example, by making data collection and analysis transparent and maintaining separation between empirical evidence and interpretive claims (Martinsuo & Huemann, 2021; Schulze et al., 2026).

Three methods bolstered credibility. First, multiple roles were included to reduce reliance on a single perspective. Second, the same predefined indicators were applied to ensure consistency across interviews. Third, mapping rules were outlined to ensure that all labels could be grounded back in interview evidence and, where available, operational artifacts. Where participants described practices as informal or manual, these were coded as reactive since standards describe proactivity in relation to standardized workflows, coordinated communication, and operationalized incident response (Zhong et al., 2024). For example, monitoring and centralized analysis (e.g., log consolidation and actionable alerting) were considered stronger evidence of proactive detection capability than ad hoc local checks (Younus & Alanezi, 2023). In the resource area, claims on prioritization and budgeting were scored more strongly if they aligned with governance routines underpinned by repeated measurement for decision-making, as opposed to one-off justifications (Herath et al., 2022).

To minimize the risk of disclosure through adjustment, we enforced ethical approaches that enable continued meaningful analysis. The organization and participants were anonymized by role; identifying information such as product or partner names, system endpoints, and configuration details that could be misused or create reputational harm has been omitted from the paper. Results are reported only with the granularity necessary to support benchmark comparison and omit operationally sensitive details that may contribute to exploitability. Such level-of-detail restraint is particularly important in studies that detect third-party dependencies, which can transmit shocks at the focal organization well beyond its immediate and external partners (Li & Xu, 2021; Wang & Xu, 2026).

RESULTS AND DISCUSSION

In order to generate the results, a systematic mapping of respondent evidence was conducted, aligning responses with paired reactive and proactive posture indicators. Findings are structured across three capability domains: incident response and strategy; budget allocation and resource administration; and security infrastructure and layered defense.

All domains were assessed using consistent, observable criteria to ensure comparability, avoiding unequal rigor across areas. To contrast stated intentions with structural constraints affecting feasibility beyond immediate operational considerations and potential future service roadmap scenarios, a five-year outlook is also provided; however, it should be interpreted as directional context rather than a binding commitment or precise forecast. Posture distribution across domains is summarized in Table 2. This analysis begins with incident response and strategy: detection and coordination patterns directly determine the speed of threat recognition and containment, and whether incidents result in sustained operational improvements when integrated with actionable monitoring practices (Younus & Alanezi, 2023).

Table 2. Posture Summary Across Domains

Domain	Predominantly Reactive	Mixed	Predominantly Proactive
Incident response and strategy	4	0	0
Budget allocation and resource management	2	2	0
Security infrastructure and layered protection	1	3	0

source: research data

Table 3. Comparison of Incident Response and Strategy

Criterion	Reactive posture indicators	Proactive posture indicators	Company X practice	Assessment
Response time	1. Limited real time alerts delay response initiation (Nitz et al., 2025; Tariq et al., 2025). 2. Triage stays manual due to noisy alerts (Nitz et al., 2025; Tariq et al., 2025) 3. No procedures slows containment decisions (Nitz et al., 2025).	1. Central logs improve early warning and speed (Fredrick et al., 2023; Kamble & Dhotre, 2025). 2. Correlation prioritizes alerts and escalates threats (Fredrick et al., 2023; Tariq et al., 2025). 3. SIEM and playbooks support faster containment (Fredrick et al., 2023; Nitz et al., 2025)	1. It responds to complaints, not real time alerts. 2. Triage is manual investigation and validation. 3. Procedures facilitate isolation, recuperation, and tracking.	**Predominantly reactive**.
Detection mechanisms	1. Fragmented telemetry causes fragmented operational visibility (Fredrick et al., 2023; Tariq et al., 2025) 2. Manual reviews replace continuous monitoring practices (Nitz et al., 2025; Tariq et al., 2025). 3. Large logs raise late detection risk (Kamble & Dhotre, 2025).	1. Continuous telemetry collected into centralized tool (Tariq et al., 2025). 2. Correlation detects anomalies and triggers alerts (Fredrick et al., 2023;Tariq et al., 2025) 3. Dashboards and rules support timely decisions (Kamble & Dhotre, 2025).	1. There is no organization-wide dedicated monitoring system. 2. Detection is after reports, not a continuous monitoring baseline. 3. We monitor activity logs and anomaly warnings.	**Predominantly reactive**.
Collaboration	1. Varying maturity hinders standardized response execution (Nitz et al., 2025). 2. Unclear roles reduce repeatable coordination (Nitz et al., 2025). 3. Sharing is inconsistent across incident	1. Defined responsibilities improve coordination accountability (Ahmad et al., 2021; Nitz et al., 2025). 2. Lifecycle based sharing builds shared understanding	1. During incidents, coordination is both ad hoc and informal. 2. Responsibilities not clear; complaints sent along unscreened. 3. Incident coordination involves third parties	**Predominantly reactive**.

Criterion	Reactive posture indicators	Proactive posture indicators	Company X practice	Assessment
	phases (Nitz et al., 2025).	(Nitz et al., 2025). 3. Analysts validate alerts and execute responses (Kamble & Dhotre, 2025).		
Post-incident reviews	1. Lessons learned are inconsistently institutionalized (Nitz et al., 2025). 2. Follow up actions lack traceable metrics (Patterson et al., 2023). 3. Reporting is weak without systematic mechanisms (Fredrick et al., 2023).	1. Reviews feed improvements into preparation practices (Nitz et al., 2025). 2. Follow-ups are tracked using measurable targets and assigned owners (Patterson et al., 2023). 3. Auditing supports documentation and continuous improvement (Fredrick et al., 2023).	1. That is not formal, and usually not systematized. 2. evaluation done to prevent it from happening again.	**Predominantly reactive**.

source: research data

Incident Response and Strategy

Incident response capability is critical to minimizing operational disruption and enabling timely recovery following security events (Naseer et al., 2023). Increasingly, effective handling relies on coordination and information exchange under time pressure, especially when investigations involve multiple roles and third parties (Zhong et al., 2024). Minimizing the detection-to-recovery time can mitigate multiple impact classes (Furnell et al., 2020; Liu & Babar, 2026), as response and recovery activities make significant contributions to overall costs associated with breaches.

In summary, the incident response strategy as well as strategy in this study is evaluated using four observable criteria: (i) time to respond; (ii) detection; (iii) collaboration to contain; and (iv) post-incident reviews (see Table 3). Each criterion is operationalized through paired reactive versus proactive indicators to elucidate opposing patterns of alert-driven vs. symptom-driven response, centralized vs. fragmented visibility, structured vs. ad hoc coordination, and standardized vs. informal learning (Zhong et al., 2024).

Overall, interview evidence suggests Company X is still largely reactive when assessed across all four criteria. The response is usually reactive, based on user reporting or operational symptoms, and it occurs at a slower pace with periodic manual triaging of issues rather than alert-driven prioritization. Similarly to the trends observed in Table 3, reviewed evidence does not support any centralized telemetry or risk-threshold detection mechanisms that enable earlier triage and containment, resembling more manual, post-impact discovery than analytics-enabled continuous monitoring (Naseer et al., 2023).

The October 2024 incident that impacted an API-facing reporting function is another example of these dynamics. An operational disruption was observed first, though mitigation required collaboration with a third-party organization (Li & Xu, 2021; Wang & Xu, 2026),

suggesting that collaborative action de facto is taken when needed. On the other hand, Table 3 also indicates that there were no playbooks structured with defined roles, standardized coordination artifacts, and routine post-incident outputs. As a result, response time and repeatability seem to be driven more by people- and event-specific coordination than defined workflows and learning steps, leading to what can become an almost stubbornly reactive stance in both incident defense and offensive initiatives (Zhong et al., 2024).

Budget Allocation and Resource Management

Budgeting and resourcing remain at the core, as cybersecurity risk translates not just to technical but also economic outcomes: incidents have direct and indirect costs, with organizations often underestimating the total expense when planning controls and recovery capacity (Furnell et al., 2020; Liu & Babar, 2026). This challenge becomes exacerbated when programs are evaluated only in terms of short-term spending visibility rather than governance-related performance measurement, which can undermine how investments are justified and sustained over time (Herath et al., 2022). In SMEs or MSEs, the tension is greater, as security is often seen as a tax while operational budgets and specialist skills are scarce, leading decisions toward deferment or low spend.

Table 4. Comparison of Budget Allocation and Resource Management

Criterion	Reactive posture indicators	Proactive posture indicators	Company practice X	Assessment
Planning orientation	1. Wait and see until signals (Herath et al., 2022; Lindkvist et al., 2025). 2. Limited resources cause episodic planning decisions (Herath et al., 2022). 3. Weak postaudit enables biased optimistic proposals (Dong et al., 2021; Herath & Herath, 2008; Schulze et al., 2026).	1. Staged roadmap uses learning and postaudit (Dong et al., 2021; Herath & Herath, 2008; Schulze et al., 2026). 2. Valuation includes proposals (Dong et al., 2021; Herath & Herath, 2008; Schulze et al., 2026). 3. Portfolio sequencing maximizes value under constraints (Sawik & Sawik, 2022).	1. Reviews are ad-hoc and not uniformly institutionalized. 2. This evaluation is done to avoid recurrence.	Predominantly reactive.
Funding cadence	1. Budget limits prevent assured security levels (Dong et al., 2021; Herath & Herath, 2008; Schulze et al., 2026). 1. Weak governance weakens spend to capability link (Herath et al., 2022; Mohammad et al., 2026) . 2. Overconfidence	2. Governance converts spending into capability growth (Herath et al., 2022; Mohammad et al., 2026) . 3. Service portfolio metrics support recurring	1. There is no separate budget for risk management 2. Security spending decisions not proven in government processes for repeat purchases.	Mixed.

Criterion	Reactive posture indicators	Proactive posture indicators	Company practice	X	Assessment
	sustains chronic underfunding (Dong et al., 2021; Herath & Herath, 2008; Schulze et al., 2026).	allocation (Carvalho et al., 2025; Jardine, 2018). 4. Training is sustained when effectiveness metrics justify spend (Chaudhary et al., 2022; Qin et al., 2025).	3. Maintain a recurring maintenance budget for infrastructure requirements.		
Decision basis	1. Politics and constraints override technical reasoning (Dong et al., 2021; Herath & Herath, 2008; Schulze et al., 2026). 2. Overconfidence reduces investment and outcomes (Dong et al., 2021; Herath & Herath, 2008; Schulze et al., 2026). 3. Missing denominators make metrics misleading (Carvalho et al., 2025; Jardine, 2018).	1. Model losses and attacker strategic interaction (Gao et al., 2023). 2. Normalize measures to avoid misleading metrics (Carvalho et al., 2025; Jardine, 2018). 3. Portfolio selection uses expected value benefits (Sawik & Sawik, 2022).	1. Other needs prioritized over risk reduction in budget 2. The decisions encompass intended audits and training		Predominantly reactive.
Resourcing model	1. Limited capacity constra (Romanosky, 2016; Saad, 2026). Operational excelle. 2. No attacker modeling weakens investment analysis (Gao et al., 2023; Wang et al., 2024). 3. No training policy keeps skills uneven (Chaudhary et al., 2022; Qin et al., 2025).	1. Governance backed spending builds capability over time (Herath et al., 2022; Mohammad et al., 2026) . 2. Governance defines routines roles and metrics (Herath et al., 2022; Mohammad et al., 2026). 3. Training policy strengthens human security capability (Chaudhary et al., 2022; Qin et al., 2025).	1. Risk work is contingent on available team capacity and coordination. 2. No specific risk training programme is described. 3. Secure practice re-freshers and briefings.		Mixed.

source: research data

To illustrate this reactive and proactive pattern contrast, we evaluate budgeting and resource management using four criteria summarized in Table 4, planning orientation, funding cadence, decision basis, and resourcing model. For each criterion, the indicators are operationalized by means of a paired contrast between investment pathways that reflect planned, repeatable, risk- and cost-informed decisions versus ad hoc, episodic, constraint-driven, adjust-on-the-fly decisions and informal resourcing practices. This framing is in line with studies indicating that planning often takes a back seat to budget pressure and complexity, but structured budgeting and a phased path of investment supported by cost–benefit reasoning could assist SMEs in making well-informed decisions regarding cybersecurity investments . It aligns with literature on investment decision-making that explores how security investments can be allocated under constraints, uncertainty, and in the face of strategic attacker–defender interactions (Gao et al., 2023), as well as approaches that explore non-isolated purchasing of controls when trying to maximize value from cybersecurity investments (Sawik & Sawik, 2022).

Interviews were conducted to ensure that the sample is representative of Company X, where a common finding was that Company X is positioned somewhere between ad hoc and proactive. Security work appears consumed in enginering delivery and operational work, as shown in Table 4, indicating baseline completion aligned with input data. However, the review of evidence does not support that there was a phased roadmap with clearly defined sequencing in place and/or an organization-wide stable cadence for assurance, monitoring, and training that would indicate sustained program funding. This “planned-but-lightweight” approach is prevalent in cases where security does not have strategic salience, and near-term limitations tend to govern decision-making (Lindkvist et al., 2025), and where governance-oriented measurement routines and executive review practices are too weak to maintain programmatic continuity (Herath et al., 2022).

In general, Company X seems to be more successful than not in evolving its resource outlays such that they go beyond a state of just-in-time reactive provisioning; yet what publicly available evidence suggests does not rise to a standard where security investment reflects explicit risk and cost variables as part of appropriately staged capability delivery and cadence throughout the organization. What is often missing in practice, therefore, is not a separate budget line (though it could be added), but rather a reasoning logic for how to finance certain things first and why these are more important than other types of spending and on what cycle. Lacking this decision-making logic, organizations all too easily revert to post-incident vigilance (and are less capable of accounting for the wider incident cost footprint previously noted in (Furnell et al., 2020; Liu & Babar, 2026). Such logic, in the presence of constraints, can be made explicit through a portfolio and staged investment perspective that helps identify which control sets generate the marginally highest yield in value for process improvement, and how decisions should adjust with new learnings from outcomes (Sawik & Sawik, 2022).

Security Infrastructure and Layered Protection

Security layers and infrastructure impact an organization’s ability to prevent, detect, and contain threats as services scale and integrated components become more critical in their workflows. In practice, the infrastructure posture is important as it relates to incident detection are incidents detected early owing to strong visibility and monitoring, or only after operational impacts are felt, which could further exacerbate downstream response effort (Furnell et al., 2020; Liu & Babar, 2026). This becomes particularly challenging for cloud-delivered services, where security control responsibility and ownership are shared between provider and customer domains. This can lead to confusion and gaps in coverage unless the roles of both parties are made explicit, specifying which controls are expected from whom, and ensuring that evidence of monitoring is part of continuous operationalization (Chauhan & Shiaeles, 2023), based on continuous assurance approaches focusing on automated collection of evidence in a traceable way for cloud-based services (Suhonen & Martínez, 2023).

This section therefore assesses the four infrastructure criteria in Table 5 to provide a comparison of reactive and proactive patterns based on observable evidence. These include preventative baseline controls, observability and telemetry, containment readiness to manage

blast radius, and an operational cadence for periodic control review. The stability of capability means maturity is scored not just on whether controls exist or are implemented, but on how relevant and consistently those controls are measured and reported over time (Belkina et al., 2025; Le & Hoang, 2016) These also align with roadmap-based guidance that stresses more foundational, incremental capability building for resilience as opposed to one-shot fixes (Kumar Jain et al., 2024). Centralized monitoring, correlation, and alerting are considered differentiators for observability in the benchmark because they allow anomalies to be detected earlier in operational environments so that triage can occur in a timely manner (Kamble & Dhotre, 2025), while SIEM-like log aggregation and analysis are proven ways of operationalizing (Younus & Alanezi, 2023).

These interviews showed that Company X has several point-solution preventive capabilities at the application and operational layer (e.g., rate limiting, input validation, encryption, CI/CD scanning, secrets management, and backup and restore testing through DRP) implemented as summarized in Table 5, with relatively stronger prevention coverage than the organization's detection and routinized review layers. Instead, monitoring is identified as weak and ad hoc, with limited visibility no centralized telemetry or logging, nor any automated alerting as a pervasive capability in the examined evidence. Why this gap matters: analytics-infused monitoring is often seen as a prerequisite for providing rapid feedback and adaptation during the early provisioning phase of incident response, while strong monitoring plays an essential role in delivering SaaS trust and control expectations at scale (Naseer et al., 2023; Younus & Alanezi, 2023). It is also more relevant when central visibility concerns are amplified across boundaries (Li & Xu, 2021; Wang & Xu, 2026), as third-party dependencies can extend exposure beyond an individual component.

The evidence under review also points to a poor state of containment readiness and a weak cycle for regular reviews. Table 5 does not show clear segmentation or isolation boundaries that could contain blast radius, so stronger statements of containment maturity cannot be made based on this data. Likewise, there is no indication that a periodic control review cadence has become standard. These could include, but are not limited to, an ongoing vulnerability management cadence that periodically reviews and monitors the status of remediation activities until closure. This trend aligns with maturity-oriented perspectives that suggest that when governance and operational routines cannot be consistently patterned across roles and over time, capability remains bounded (Belkina et al., 2025; Le & Hoang, 2016). This is also in agreement with a dependency and supply-chain perspective in which structural dependencies are exposed across multiple systems, increasing exposure to any vulnerable system and driving up complexity and containment design costs, while reducing repeatable assurance as a system scales (Li & Xu, 2021; Wang & Xu, 2026).

Table 5. Comparison of Security Infrastructure and Layered Protection

Criterion	Reactive posture indicators	Proactive posture indicators	Company X practice	Assessment
Preventive baseline controls	1. Ad hoc controls without baseline visibility (Tuyishime et al., 2023). 2. Unclear responsibilities cause coverage gaps (Chauhan & Shiaeles, 2023). 3. Layer mapping inconsistent, verification remains weak (Chauhan & Shiaeles, 2023; Suhonen & Martínez, 2023).	1. Baseline anchored to shared responsibility boundaries (Chauhan & Shiaeles, 2023). 2. Control visibility maintained for audits (Suhonen & Martínez, 2023). 3. Formal mapping enables routine verification (Suhonen & Martínez, 2023).	1. Server side filtering and automated rejection rules exist. 2. Access control, input validation, and encryption are implemented.	**Mixed**.

Criterion	Reactive posture indicators	Proactive posture indicators	Company X practice	Assessment
Observability and telemetry	1. No centralized logs, monitoring remains fragmented (Kamble & Dhotre, 2025). 2. Alerts lack actionable correlation rules (Fredrick et al., 2023; Tariq et al., 2025) 3. No dashboards slow detection and triage (Gupta et al., 2024; Kamble & Dhotre, 2025).	1. Centralize telemetry and correlate events (Fredrick et al., 2023; Tariq et al., 2025) 2. Dashboards and alerts speed triage (Kamble & Dhotre, 2025). 3. Monitoring actively supports response actions (Kamble & Dhotre, 2025).	1. Dedicated monitoring system not confirmed across organization. 2. System events and change traces are recorded.	**Predominantly reactive**.
Containment readiness	1. Procedures not structured for timely containment (Nitz et al., 2025). 2. Playbooks absent actions remain unsequenced (Nitz et al., 2025). 3. No security zoning, isolation becomes harder (Gupta et al., 2024).	1. Procedures guide containment remediation and recovery (Nitz et al., 2025). 2. Playbooks enable repeatable containment execution (Nitz et al., 2025). 3. Security zoning limits incident spread (Gupta et al., 2024).	1. Isolation steps are executed during third party incidents. 2. Incident procedure includes evidence collection and notification.	**Mixed.**
Assurance cadence	1. Scanning and assessment not institutionalized (de Bruin & von Solms, 2015; Gupta et al., 2024). 2. Patching manual and inconsistently executed (de Bruin & von Solms, 2015; Gupta et al., 2024). 3. Policy based cadence remains unstable (de Bruin & von Solms, 2015; Gupta et al., 2024).	1. Recurring scans and penetration tests planned (de Bruin & von Solms, 2015; Gupta et al., 2024). 2. Continuous monitoring suptivenes (Kamble & Dhotre, 2025). 3. Systematic patching verified through closure (de Bruin & von Solms, 2015; Gupta et al., 2024).	1. Automated dependency scanning and periodic review exist. 2. Backups and recovery tests are performed routinely.	**Mixed.**

source: research data

Projected Positioning and Investment Intent

Participants spoke to a growth strategy that favors market penetration and competition over large-scale investment in cybersecurity, a trend often found among SMEs/MSEs where constrained financial resources and intrusion-related capacity constraints tend to direct expenditure towards revenue-earning activities and operational delivery (Gao et al., 2023; Lindkvist et al., 2025). Although external partners might alleviate vulnerability in certain domains, third-party reliance cannot replace in-house preparedness, as fundamental features like surveillance, systematic incident response processes, and repeatable assurance are still lacking (McCormack & Bendechache, 2026; Monev, 2021), especially given that risks associated with third

parties can diffuse and complicate response across interconnected offerings (Li & Xu, 2021; Wang & Xu, 2026).

Table 6 summarizes the five-year outlook across these three domains as an evidence-based, rather than definitive, trajectory. The trajectory is presented as a conditional outlook under relatively consistent constraints and operating patterns and should not be interpreted as a deterministic forecast. Unless there is a shift toward established continuous monitoring supported by centralized telemetry and alerting, the implementation of consistent incident routines with clear roles and learning loops, and planned, stepped security investment that can be consistently justified at executive levels within Company X, Company X will continue to be predominantly reactive. In roadmap-oriented work, improved cybersecurity is framed as building capabilities over time through an iterative sequence of activities and levels of ownership sustained by ongoing investment, rather than a set of isolated, one-off initiatives (Kumar et al., 2024). In practice, such programs are often accompanied by aligned governance routines and decision-oriented metrics that allow prioritization to be made overtly and repeatably across review cycles (Herath et al., 2022).

At that stage, penetration testing was proposed as a possible next step and is therefore listed in Table 6 as an optional proactive assurance activity. However, planning and investment frameworks demonstrate that assurance is most valuable when coupled with an operational feedback loop a process by which findings are triaged, turned into prioritized work, checked for completion, and reviewed via repeatable performance evaluation practices that improve daily readiness (Liu et al., 2025). Absent additional meta-detection capabilities such as centralized telemetry and alerting, structured incident routines, penetration testing alone has limited impact on improving detection or response repeatability (Zhong et al., 2024). Moreover, under budget constraints, a staged or portfolio method can also be used to determine which combination of controls will create the greatest marginal benefit and in what order improvements should be sequenced (Gao et al., 2023; Sawik & Sawik, 2022).

As shown in Table 6, incremental prevention improvements especially low-friction engineering controls are plausible, while visibility and standardized response practices may lag behind unless investment intent is more programmatic. The projection is an evidence-based expectation derived from current signals and regular SME/ MSE constraints, not a definitive result of planned initiatives (Lindkvist et al., 2025). It resonates with decision-oriented perspectives that conceptually treat security investment as iterative capability creation under uncertainty rather than one-time optimization (Lindkvist et al., 2025). Table 6 is not a firm or definitive commitment (or deterministic forecast) but rather a conditional trajectory of broadly comparable operating patterns over time.

Table 6. Conditional Five-Year Trajectory Under Current Constraints

Domain	Reactive trajectory signals	Proactive trajectory signals	Company X projected trajectory (5-year)	Projected classification
Incident response and strategy	1. Monitoring stays decentralized, triage remains slower (Kamble & Dhotre, 2025). 2. Playbooks not institutionalized, containment less repeatable (Nitz et al., 2025). 3. Lessons learned rarely improve preparation routines (Nitz et al., 2025).	1. Central correlation becomes routine for triage (Kamble & Dhotre, 2025). 2. Procedures enable repeatable containment execution (Nitz et al., 2025). 3. Lessons learned feed	1. Without monitoring investment, alert driven detection unlikely. 2. Informal coordination patterns may persist under constraints. 3. Procedures may remain but scaling standardization	**Predominantly reactive** (projected).

Domain	Reactive trajectory signals	Proactive trajectory signals	Company X projected trajectory (5-year)	Projected classification
		preparation improvements (Nitz et al., 2025).	is unclear.	
Budget allocation and resource management	1. Budget limits constrain recurring security allocation (Gao et al., 2023). 2. Weak governance weakens spend capability linkage (Carvalho et al., 2025; Jardine, 2018). 3. Prioritization remains and ptimized (Sawik & Sawik, 2022).	1. Portfolio sequencing maximizes value under constraints (Sawik & Sawik, 2022). **2.** Governance and metrics stabilize review cadence (Herath et al., 2022; Mohammad et al., 2026). 3. Measurement design fixes denominator problems (Carvalho et al., 2025; Jardine, 2018).	1. Dedicated risk budget likely remains limited short term. 2. Maintenance budget likely continues for core infrastructure. 3. Governance cadence and metrics routines remain uncertain.	**Predominantly reactive** (projected).
Security infrastructure and layered protection	1. Fragmented monitoring persists, alerts not baseline (Kamble & Dhotre, 2025). 2. Shared responsibility not operationalized into baselines (Chauhan & Shiaeles, 2023). 3. Assurance irregular (de Bruin & von Solms, 2015; Gupta et al., 2024; Suhonen & Martínez, 2023).	1. Centralized correlation becomes ability (Kamble & Dhotre, 2025). 2. Shared responsibility drives standardized verification baselines (de Bruin & von Solms, 2015; Gupta et al., 2024; Suhonen & Martínez, 2023)	1. Existing technical controls likely continue incrementally. 2. Organization wide monitoring system remains uncertain. 3. Automated scanning likely continues if pipeline maintained.	**Predominantly reactive** (projected).

source: research data

Discussion

Adequacy of Reactive Posture and Practical Transition Path

Scoring across incident response, budgeting, and infrastructure data yields evidence that Company X exhibits a largely reactive posture. The response is reactive to symptoms; monitoring is periodic/manual with limited visibility; coordination exists but is frequently informal; and post-

incident follow-up is ad hoc rather than systematic. Comparison across domains/criteria is summarized in Tables 2 to 5 and confirms these cross-domain patterns. This profile is also consistent with the existing state of play across many resource-constrained SMEs and MSEs, where limited specialist capacity, coupled with competing growth priorities, keeps security-related work entrenched in a permanent cycle of day-to-day delivery and fix-as-needed activities, as opposed to ongoing capability building (Lindkvist et al., 2025). Due to the increasing complexity of incidents and integration dependencies, manual analysis and ad hoc processes can (Furnell et al., 2020; Liu & Babar, 2026).

The five-year forecast must be read as conditional not deterministic. For example, based on Table 6, Company X would remain purely reactive and will continue to do so as long as restrictions and decision-making (1), framed by a pre-2020 environment, remain unchanged. Absent a true movement toward centralized telemetry and alerting, standardized incident routines, and a staged investment path with clear ownership and cadence, improvement is unlikely to materialize. Instead, the projection represents the presence or absence of commitment signals in the evidence examined, not an assertion that improvement is impossible. In an MSE SaaS POS context with third-party dependencies where coordination of external escalation cannot compensate for internal capacity when early detection, structured escalation, and repeatable learning loops are underdeveloped (McCormack & Bendechache, 2026; Monev, 2021) this conditional framing matters. Budget constraints further shape sustainability, as capability gains tend to be less durable when funding is episodic rather than planned as recurring program work, and are instead strengthened through governance cadence and routine measurement review (Gao et al., 2023).

A small set of capabilities most clearly separates a reactive posture from a more proactive stance, per the benchmark rubric in this case. The first is centralized observability telemetry and log aggregation with risk-threshold alerting. This reduces dependence on self-reported symptoms and enables more rapid front-line assessment in an environment of further-recognized patterns, including analytics-enabled incident response (Naseer et al., 2023), while also being positioned as a trust and control enabler in SaaS contexts. It aligns with SIEM-centric monitoring approaches, where correlation and actionable alerting serve as operational enablers of detection and triage (Younus & Alanezi, 2023).

Second, when an organization establishes standard incident response routines with clearly defined roles, escalation paths, and shared coordination artifacts, it reduces reliance on individual knowledge and enables repeatable outcomes. This aligns with recent research on collaborative incident response, which highlights challenges in coordination and follow-through (Zhong et al., 2024). Third, as an operational assurance loop, iterative vulnerability management and hardening where findings are tracked through to confirmed closure strengthens maturity over time. Capability, in this framing, is defined by reliable and sustained application rather than the one-off presence of activity (Belkina et al., 2025; Le & Hoang, 2016), which better replaces episodic post-incident security cycles often triggered under budget constraints. When review cadence and closure become verifiable parts of governance routines rather than informal practice, sustained assurance becomes significantly easier to maintain (Herath et al., 2022).

One possible transition path for an MSE, reflecting the salient differences here, is not a transformation but a set of high-leverage incremental evolutions. Establishing at least a minimal observability layer for every mission-critical service (centralized logging with alerting based on appropriate signals) reduces reliance on symptom-led detection and decreases manual effort in preliminary incident assessment (Naseer et al., 2023), while also improving operator visibility and control over day-to-day SaaS operations (Abdelrazek et al., 2015; Kamble & Dhotre, 2025). Simultaneously, lightweight formalization improves repeatability. This may include basic playbooks with clearly defined roles and step-by-step post-incident review templates that capture actions taken, ownership, deadlines, and metric verification points, enabling learning loops to better support collective incident response efforts (Zhong et al., 2024).

Over time, these changes should be supported with baseline measures that reduce blast radius and a valid (Belkina et al., 2025; Le & Hoang, 2016). A minimally staged investment path along with sequencing, allocation logic, and cadence that does not default to post-incident urgency

will help sustain progress. Planning-oriented research has shown that, under this methodology, improvements become more sustainable because capability development is embedded within constraints rather than treated as a one-time initiative (Kumar et al., 2024). When budgets are tight, a portfolio view can help stakeholders focus on a shortlist of controls that yield the highest marginal return in both security improvement and feasibility for staged rollout (Gao et al., 2023; Sawik & Sawik, 2022).

CONCLUSION

Using a rubric fashioned from earlier literature, this study then assessed Company X an emerging MSE SaaS POS provider in Indonesia with dependence on third-party integrations against a reactive and proactive posture divided across three capability domains: incident response (including strategy, budgeting, and asset allocation) as well as security covering physical to layered defenses. Company X is still largely reactive, as characterized in the assessment, with respect to those capabilities most conducive to day-to-day readiness. Detection is mostly reactive, relying on manual "look-and-feel" checklists, audited ad hoc rather than telemetry and alerts from a centralized source. Incident coordination and post-incident learning are functional but not always consistent.

Placing it in this context, resource allocation is shaped more by abstract operational requirements than by a clear, phased investment strategy focused on developing security capabilities over time. Thus, the most consequential differences between reactive, mixed, and more proactive postures have less to do with stated intent and more to do with what is actually in place as routine day-to-day practice across observability and hypothesis testing. This strongly favors centralized telemetry and alerting, incident handling routines that include defined roles and escalation paths, and a continuous learning loop supporting capability building underpinned by planned resource allocation and recurrence cadence.

The identified gaps are priorities that can realistically be addressed within MSE constraints and would have high impact. The most realistic transition focuses on incremental, high-payoff improvements rather than a single large-scale transformation. First, it starts with a minimal viable setup: centralized logging, telemetry, and alerting for critical services. Next, it introduces lightweight incident workflows with traceable post-incident outputs as actionable items, including ownership and due dates for verification. It then reinforces containment readiness and establishes a rhythm of repeatable assurance activities such as cyclical vulnerability management and hardening routines tracked to verified closure. Underlying this is a selective degree of proactive trait discovery and baseline recovery readiness for Company X; however, these aspects are unlikely to meaningfully shift systemic outcomes associated with symptom-driven discovery or personnel-driven response in the absence of stronger observability that enables repeatable operating routines.

ACKNOWLEDGEMENT

The authors thank the interview participants and the anonymized case organization (Company X) for their time, cooperation, and access to supporting materials. This study received no external funding. The views expressed in this paper are solely those of the authors.

AUTHOR CONTRIBUTION STATEMENT

Ryan Adhi Nugraha: Conceptualization, methodology, investigation, data collection, formal analysis, cybersecurity risk assessment, writing – original draft preparation, and project administration. Muhammad Hafizhuddin Hilman: Research design, data analysis, validation, literature review, interpretation of findings, and writing – review and editing. Setiadi Yazid: Supervision, methodological guidance, validation, critical review of the manuscript, and academic oversight. Eko Yon Handri: Supervision, strategic evaluation of cybersecurity frameworks, manuscript review, final approval, and overall research guidance. All authors have read and approved the final version of the manuscript. The authors agree to be accountable for all aspects of the work and ensure the integrity, accuracy, and reliability of the research findings.

REFERENCES

Abdelrazek, M. A., Grundy, J., & Ibrahim, A. S. (2015). Improving Tenants' Trust in SaaS Applications Using Dynamic Security Monitors. *2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS)*, 70–79. https://doi.org/10.1109/ICECCS.2015.18

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Alpi, K. M., & Evans, J. J. (2019). Distinguishing case study as a research method from case reports as a publication type. *Journal of the Medical Library Association*, *107*(1). https://doi.org/10.5195/jmla.2019.615

Belkina, M., Daniel, S., Nikolic, S., Haque, R., Lyden, S., Neal, P., Grundy, S., & Hassan, G. M. (2025). Implementing generative AI (GenAI) in higher education: A systematic review of case studies. *Computers and Education: Artificial Intelligence*, *8*, 100407. https://doi.org/10.1016/j.caeai.2025.100407

Berisha, G., & Pula, J. S. (2015). Defining Small and Medium Enterprises: a critical review. In *Academic Journal of Business, Administration, Law and Social Sciences*, 1(1). www.iipccl.org

Carvalho, N., Adão, T., Morais, R., Costa, A. R., & Peres, E. (2025). Cybersecurity in Precision Agriculture: a short review and a practical status assessment over mySense IoT-based platform. *Procedia Computer Science*, *256*, 255–266. https://doi.org/10.1016/j.procs.2025.02.119

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, *8*(1). https://doi.org/10.1093/cybsec/tyac006

Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*, *3*(3), 422–450. https://doi.org/10.3390/network3030018

de Bruin, R., & von Solms, S. H. (2015). Modelling Cyber Security Governance Maturity. *2015 IEEE International Symposium on Technology and Society (ISTAS)*, 1–8. https://doi.org/10.1109/ISTAS.2015.7439415

Dong, K., Lin, R., Yin, X., & Xie, Z. (2021). How does overconfidence affect information security investment and information security performance? *Enterprise Information Systems*, *15*(4), 474–491. https://doi.org/10.1080/17517575.2019.1644672

Fredrick, S., Singh, P., & V, R. (2023). Cyber Threat Monitoring and Incident Response with IntelliWatch SIEM. *2023 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, 209–215. https://doi.org/10.1109/ICSCNA58489.2023.10370155

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, *2020*(12), 6–12. https://doi.org/10.1016/S1361-3723(20)30127-5

Gao, X., Qiu, M., Wang, Y., & Wang, X. (2023). Information security investment with budget constraint and security information sharing in resource-sharing environments. *Journal of the Operational Research Society*, *74*(6), 1520–1535. https://doi.org/10.1080/01605682.2022.2096506

Gupta, D., Elluri, L., Jain, A., Moni, S. S., & Aslan, O. (2024). Blockchain-Enhanced Framework for Secure Third-Party Vendor Risk Management and Vigilant Security Controls. *2024 IEEE International Conference on Big Data (BigData)*, 5577–5584. https://doi.org/10.1109/BigData62323.2024.10825025

Herath, H. S. B., & Herath, T. C. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems*, *25*(3), 337–375. https://doi.org/10.2753/MIS0742-1222250310

Herath, T. C., Herath, H. S. B., & Cullum, D. (2022). An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-022-10246-9

Jardine, E. (2018). Mind the denominator: towards a more effective measurement system for

cybersecurity. *Journal of Cyber Policy*, *3*(1), 116–139. https://doi.org/10.1080/23738871.2018.1472288

Kamble, A., & Dhotre, P. (2025). Centralized Security Monitoring for Effective Threat Detection and Analysis. *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)*, 1–6. https://doi.org/10.1109/ICTBIG68706.2025.11323853

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2023). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. *ACM Transactions on Privacy and Security*, *26*(1), 1–29. https://doi.org/10.1145/3546068

Kumar J. Y., Dhaarna, S. R. C. A., Johrawanshi, A., Gupta, M., Choudhary, D. K., & Pandey, A. (2024). Cybersecurity Frameworks: A Roadmap for Business Resilience. *2024 International Conference on Cybernation and Computation (CYBERCOM)*, 102–108. https://doi.org/10.1109/CYBERCOM63683.2024.10803234

Le, N. T., & Hoang, D. B. (2016). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, 1–7. https://doi.org/10.1109/PCCC.2016.7820663

Lindkvist, A., Hoglund, E., & Djebbar, F. (2025). Cybersecurity Practices, Challenges and Posture in Small and Medium Enterprises: A Survey-Study in Sweden. *European Conference on Cyber Warfare and Security*, *24*(1), 838–847. https://doi.org/10.34190/eccws.24.1.3579

Liu, C., & Babar, M. A. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, *51*(1), 62–92. https://doi.org/10.1177/03128962241293658

Liu, M., Shore, M., Yeoh, W., Jiang, F., & Zeadally, S. (2025). Toward effective cybersecurity management: a hierarchical process model with performance assessment. *Journal of Cybersecurity*, *11*(1). https://doi.org/10.1093/cybsec/tyaf020

Li, Y., & Xu, L. (2021). Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *International Journal of Production Research*, *59*(4), 1216–1238. https://doi.org/10.1080/00207543.2020.1721591

López-Ortega, E., Canales-Sanchez, D., Bautista-Godinez, T., & Macias-Herrera, S. (2016). Classification of micro, small and medium enterprises (M-SME) based on their available levels of knowledge. *Technovation*, *47*, 59–69. https://doi.org/10.1016/j.technovation.2015.10.001

Magdy E. H., & Crispm, J. (2026). Assessing Industry 4.0 adoption in Cairo SMEs: a study on manufacturing sector. *International Journal of Computer Integrated Manufacturing*, *39*(4–5), 705–726. https://doi.org/10.1080/0951192X.2025.2545481

Martinsuo, M., & Huemann, M. (2021). Reporting case studies for making an impact. *International Journal of Project Management*, *39*(8), 827–833. https://doi.org/10.1016/j.ijproman.2021.11.005

McCormack, L., & Bendechache, M. (2026). The Trustworthy AI Maturity Model (TAIMM): Integrating ethics and regulation across the AI lifecycle. *Journal of Responsible Technology*, *26*, 100156. https://doi.org/10.1016/j.jrt.2026.100156

Mohammad, M. H. G., Mohammad, A. N., Ahmad, A. A. F., Abdel, K. A. K., & Abu, H. Y. (2026). Cybersecurity spending and IT capability development: The mediating role of IT governance effectiveness. *EDPACS*, *71*(5), 82–92. https://doi.org/10.1080/07366981.2025.2564773

Monev, V. (2021). The “Self-Assessment” Method within a Mature Third-Party Risk Management Process in the Context of Information Security. *2021 International Conference on Information Technologies (InfoTech)*, 1–7. https://doi.org/10.1109/InfoTech52438.2021.9548373

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. *Computers & Security*, *135*, 103525. https://doi.org/10.1016/j.cose.2023.103525

Nitz, L., Akbari Gurabi, M., Cermak, M., Zadnik, M., Karpuk, D., Drichel, A., Schäfer, S., Holmes, B., & Mandal, A. (2025). On Collaboration and Automation in the Context of Threat Detection and Response with Privacy-Preserving Features. *Digital Threats: Research and Practice*, *6*(1), 1–36. https://doi.org/10.1145/3707651

Olipp, N., Jöbstl, L., & Woschank, M. (2026). Factors of success and challenges of the transformation

of the production and logistics system from a linear to a circular model in Austrian small and medium-sized enterprises. *Cogent Engineering*, *13*(1). https://doi.org/10.1080/23311916.2025.2599578

Oriola, O., Adeyemo, A. B., Papadaki, M., & Kotzé, E. (2021). A collaborative approach for national cybersecurity incident management. *Information & Computer Security*, *29*(3), 457–484. https://doi.org/10.1108/ICS-02-2020-0027

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, *132*, 103309. https://doi.org/10.1016/j.cose.2023.103309

Pech, M., & Vrchota, J. (2020). Classification of Small- and Medium-Sized Enterprises Based on the Level of Industry 4.0 Implementation. *Applied Sciences*, *10*(15), 5150. https://doi.org/10.3390/app10155150

Qin, Y., Yang, X., Yang, L.-X., & Huang, K. (2025). Mitigating Social Engineering Attacks Through Cost-Effective Security Awareness Training Policy. *IEEE Transactions on Network Science and Engineering*, *12*(4), 3145–3158. https://doi.org/10.1109/TNSE.2025.3556927

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, tyw001. https://doi.org/10.1093/cybsec/tyw001

Saad, M. A. T. (2026). Economic impact of cybersecurity breaches on organizational sustainability. *EDPACS*, 1–14. https://doi.org/10.1080/07366981.2025.2602630

Sawik, T., & Sawik, B. (2022). A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value. *International Journal of Production Research*, *60*(21), 6556–6572. https://doi.org/10.1080/00207543.2021.1994166

Schulze, F., Dallasega, P., Alfnes, E., & Sgarbossa, F. (2026). The mitigation effect of Industry 4.0 technologies on Lean implementation barriers in Engineer-to-Order companies: A Multiple Case Study. *Production Planning & Control*, *37*(2), 128–152. https://doi.org/10.1080/09537287.2025.2468449

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974. https://doi.org/10.1016/j.cose.2022.102974

Suhonen, T., & Martínez, C. (2023). Continuous Auditing and Continuous Certification in MEDINA – Security Auditor's View. *Open Research Europe*, *3*, 208. https://doi.org/10.12688/openreseurope.16703.1

Tariq, S., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2025). Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities. *ACM Computing Surveys*, *57*(9), 1–38. https://doi.org/10.1145/3723158

Tuyishime, E., Balan, T. C., Cotfas, P. A., Cotfas, D. T., & Rekeraho, A. (2023). Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach. *Applied Sciences*, *13*(22), 12359. https://doi.org/10.3390/app132212359

Wang, X., Li, W. W., Leung, A. C. M., & Yue, W. T. (2024). To alert or alleviate? A natural experiment on the effect of anti-phishing laws on corporate IT and security investments. *Decision Support Systems*, *179*, 114173. https://doi.org/10.1016/j.dss.2024.114173

Wang, Y., & Xu, F. (2026). Optimal cybersecurity investment with collaborative defense in scale-free supply chain networks: a stochastic game-based dynamic programming approach. *International Journal of Production Research*, 1–13. https://doi.org/10.1080/00207543.2026.2653814

Younus, Z. S., & Alanezi, M. (2023). Detect and Mitigate Cyberattacks Using SIEM. *2023 16th International Conference on Developments in ESystems Engineering (DeSE)*, 510–515. https://doi.org/10.1109/DeSE60595.2023.10469387

Zhong, C., Zaza, S., & Bartelt, V. (2024). Understanding Communication Preferences in Collaborative Cybersecurity Incident Response. *Proceedings of the 2024 Computers and People Research Conference*, 1–1. https://doi.org/10.1145/3632634.3655851