frontiers | Frontiers in Communications and Networks

TYPE Original Research
PUBLISHED 03 June 2025
DOI 10.3389/frcmn.2025.1594554

OPEN ACCESS

EDITED BY
Muriel Figueredo Franco,
Federal University of Health Sciences of Porto Alegre, Brazil

REVIEWED BY
Saadane Rachid,
École Hassania des Travaux Publics, Morocco
Touraj Khodadadi,
University of Technology Malaysia, Malaysia

*CORRESPONDENCE
Smitti Darakorn Na Ayuthaya,
smitti.dar@mahidol.ac.th

RECEIVED 16 March 2025
ACCEPTED 15 May 2025
PUBLISHED 03 June 2025

CITATION
Rattanapong P, Sukma N and Darakorn Na Ayuthaya S (2025) Determinants of cybersecurity investment in ASEAN organizations: an integrated structural equation modeling approach.
Front. Commun. Netw. 6:1594554.
doi: 10.3389/frcmn.2025.1594554

Determinants of cybersecurity investment in ASEAN organizations: an integrated structural equation modeling approach

Phasikha Rattanapong[1], Narongsak Sukma[2] and Smitti Darakorn Na Ayuthaya[1]*

[1]Technology of Information System Management Division, Faculty of Engineering, Mahidol University, Nakhonpathom, Thailand, [2]Professional Cybersecurity, Faculty of Digital, Siam Technology College, Bangkok, Thailand

This study examines the factors influencing cybersecurity investment decisions in organizations across the ASEAN region's diverse digital landscape, where varying levels of regulatory maturity and digital adoption create unique security challenges. Using structural equation modeling (SEM) with data from 317 cybersecurity and IT executives, we investigated how risk management practices, financial considerations, and cybersecurity governance and compliance affect investment patterns, both directly and through the mediating role of cybersecurity strategy. The research methodology employed a validated instrument capturing multiple dimensions of organizational practices, including threat assessment processes, budget allocation frameworks, and strategic planning approaches. Our analysis revealed that cybersecurity strategy serves as the primary determinant of investment ($\beta = 0.63$, $p < 0.001$), while being significantly influenced by financial considerations ($\beta = 0.57$, $p < 0.001$), risk management ($\beta = 0.54$, $p < 0.001$), and regulatory environments ($\beta = 0.42$, $p < 0.001$). Notably, different mediation patterns emerged across factors, with financial considerations influencing investment exclusively through strategy (full mediation), whereas risk management and governance factors affected investment both directly and indirectly (partial mediation). Further investigation through multi-group analysis uncovered significant differences between critical infrastructure and other sectors, with regulatory and risk management factors exerting stronger influence in critical infrastructure organizations. Overall, our model explains 68% of the variance in cybersecurity investment decisions, providing robust explanatory power despite the region's heterogeneity. These findings offer a comprehensive framework for understanding security resource allocation in ASEAN's diverse digital landscape and provide valuable insights for organizations seeking to optimize their cybersecurity investments. Additionally, the results inform policymakers developing regulatory frameworks that can effectively drive security enhancements while accommodating the economic and technological diversity that characterizes the ASEAN region.

KEYWORDS

cybersecurity investment, risk management, financial considerations, cybersecurity strategy, investment decision-making, organizational security

1 Introduction

The global cybersecurity landscape has undergone dramatic transformation over the past decade, with organizations, governments, and individuals facing unprecedented increases in both the frequency and sophistication of cyber threats. The magnitude and impact of cyber-attacks have grown exponentially, with significant incidents targeting critical infrastructure, financial institutions, healthcare systems, and government agencies worldwide (Pattnaik et al., 2023). Industry reports estimate that global cybercrime costs are projected to reach unprecedented levels, highlighting the substantial economic implications of cybersecurity challenges (Market Report Analytics, 2024). From ransomware attacks that paralyze operations to data breaches exposing sensitive information, the financial and reputational impacts of cyber incidents have become increasingly severe. The ASEAN region, comprising ten diverse Southeast Asian nations, faces these cybersecurity challenges within its unique socioeconomic context. As ASEAN countries experience rapid digital transformation and economic growth, they simultaneously become more vulnerable to cyber threats targeting their critical infrastructure, government institutions, businesses, and citizens. Between 2021 and 2022, cybercrime in Southeast Asia increased by 82%, with Singapore, Indonesia, Thailand, and Vietnam—the countries with the highest digitalization rates—becoming the most frequent targets (CSIS, 2023). The ASEAN Cybersecurity Cooperation Strategy (2021–2025) recognizes cybersecurity as "a key enabler of the economic progress and betterment of living standards in the digital economy" while acknowledging the larger attack surface created by rapid digitalization (ASEAN, 2023).This vulnerability is compounded by the region's significant diversity in digital maturity, regulatory frameworks, and cybersecurity capabilities. The ASEAN region exhibits substantial technological disparities, with Singapore ranking among the world's most digitally prepared nations while other member states face considerable challenges in building basic cybersecurity infrastructure (Caballero-Anthony and Gong, 2021). These differences create unique challenges for establishing consistent security approaches across the region, particularly as digital integration accelerates through initiatives such as the ASEAN Digital Masterplan 2025. Despite extensive research examining global and regional cybersecurity challenges, a significant research gap exists regarding culturally and contextually appropriate cybersecurity investment models tailored to ASEAN member states' specific characteristics. While researchers have established the importance of balanced investment approaches across technical infrastructure, governance mechanisms, and human capacity development (Hossain et al., 2023), current literature lacks empirically validated frameworks accommodating the heterogeneous regulatory environments, varying digital maturity levels, and distinct socioeconomic priorities across ASEAN countries.

This gap has particular significance as organizations throughout the region struggle to optimize investment allocations while addressing both compliance requirements and emerging threats unique to Southeast Asia's rapidly evolving digital ecosystem. Recent studies have identified several critical factors influencing cybersecurity investment, including board governance characteristics (Mazumder and Hossain, 2023), regulatory frameworks (Liu and Babar, 2024), and financial considerations (Mazzoccoli, 2023), but have not examined how these factors operate within ASEAN's specific context. To address these gaps, this study examines the following research questions:

RQ1: What factors significantly influence cybersecurity investment decisions in ASEAN organizations, and what are their relative impacts?

RQ2: How do risk management practices, financial considerations, and regulatory compliance affect cybersecurity investment both directly and through the mediating role of cybersecurity strategy?

These research questions guide our empirical investigation using structural equation modeling with data from 317 cybersecurity and IT executives across the ASEAN region. By examining both direct and indirect pathways through which key factors shape investment patterns, with particular attention to the mediating role of cybersecurity strategy, this study provides a comprehensive understanding of cybersecurity investment decision-making processes within ASEAN's diverse digital landscape.

The findings from this study offer substantial benefits to multiple stakeholders across the ASEAN region. For organizations, our research provides a contextually appropriate investment model balancing compliance requirements with proactive security measures tailored to the region's specific threat landscape. Policymakers gain evidence-based insights to develop regulatory frameworks acknowledging diverse digital maturity levels across ASEAN member states. The research also supports ASEAN's broader digital integration initiatives by enhancing regional cybersecurity resilience while accommodating economic and technological diversity within Southeast Asia. Ultimately, this study contributes to developing more secure digital ecosystems capable of supporting sustainable economic growth throughout the ASEAN community.

2 Literature review and hypothesis development

This section establishes the theoretical foundations for our research model by examining the key factors influencing cybersecurity investment decisions in the ASEAN context. We develop a comprehensive framework integrating cybersecurity risk management, financial considerations, governance and compliance, and organizational cybersecurity strategy. Based on this theoretical foundation, we propose six hypotheses that guide our empirical investigation.

2.1 Cybersecurity risk management (CRM)

Cybersecurity Risk Management (CRM) has emerged as a fundamental framework for understanding organizational security posture and investment decisions. This theoretical approach emphasizes the systematic identification, assessment, and mitigation of cybersecurity threats through structured processes that simultaneously protect organizational assets while optimizing resource allocation. Recent literature consistently demonstrates the significance of comprehensive risk management approaches in

shaping organizational security outcomes and investment priorities. Recent empirical research by Celeny et al. (2023) supports the prioritization of cybersecurity investments based on determinants of cyberattack costs, highlighting how risk assessment directly influences resource allocation decisions. Within the ASEAN context, risk management practices are particularly critical given the region's rapidly evolving threat landscape. According to Liu and Babar (2024), organizations can categorize cybersecurity risk determinants into four key groups: attributes of managers and directors, firm characteristics and policies, IT policies and practices, and institutional and environmental factors. This multidimensional framework aligns with ASEAN's Cybersecurity Cooperation Strategy 2021–2025, which emphasizes risk-based approaches to securing the region's digital infrastructure (ASEAN, 2023). Research by Melaku (2023) introduces a context-based and adaptive cybersecurity risk management framework, arguing that effective risk management must accommodate the specific organizational, cultural, and regional contexts in which it operates. This perspective is particularly relevant for ASEAN organizations navigating diverse regulatory environments and digital maturity levels. Similarly, Pattnaik et al. (2023) demonstrate through systematic analysis the substantial implications of cyber incidents for critical infrastructure and how effective risk management practices significantly reduce potential losses. Within ASEAN's digital economy landscape, where cybercrime increased by 82% between 2021 and 2022 (CSIS, 2023), risk management approaches must be calibrated to address rapidly evolving threats. The integration of cyber risk analysis within broader organizational decision-making processes has been highlighted by Rios Insua et al. (2021), who developed an adversarial risk analysis framework for cybersecurity that enables organizations to systematically evaluate threat scenarios and optimize defensive investments. For smaller enterprises across ASEAN, Tetteh and Otioma (2022) emphasize how cyber risk mitigation capabilities have measurable impacts on firm productivity and financial performance, reinforcing the economic dimensions of security decisions. These theoretical perspectives and empirical findings suggest two critical relationships: first, that risk management directly influences investment decisions by identifying security priorities; and second, that risk management shapes strategic security planning processes. Therefore, we propose:

H1: Cybersecurity Risk Management positively influences cybersecurity investments.

H2: Cybersecurity Risk Management positively influences cybersecurity strategy.

2.2 Financial considerations (FIC)

Financial Considerations (FIC) in cybersecurity investment examines how economic factors influence security decision-making within organizations. Recent research demonstrates that financial development is intrinsically linked with security risk management, as evidenced by quantitative analyses in developed economies (Kartal et al., 2022). Within ASEAN, where economic development varies significantly from Singapore's advanced economy to emerging markets like Cambodia and Myanmar, financial considerations take on particular importance in security investment decisions. The economic impact of cyberattacks in ASEAN has been significant and growing. By July 2023, economic losses from data breaches in the region had exceeded $3 million, up from $2.87 million in 2022 (Positive Technologies, 2023). These direct financial impacts create strong economic incentives for investment in preventive security measures. As noted by Mazzoccoli (2023), optimal cybersecurity investment within a mixed risk management framework requires careful analysis of expenditures against potential losses, incorporating cyber insurance as a risk transfer mechanism. Corporate investment behaviors in response to external security risks show complex patterns of expansion or retrenchment, suggesting that financial considerations significantly impact security-related resource allocation (Zhang et al., 2023). This dynamic is particularly relevant in ASEAN's diverse economic landscape, where organizations must balance cybersecurity investments against other business priorities in environments ranging from highly developed digital economies to emerging markets. The establishment of "reasonable security measures" is increasingly shaped by liability concerns and judicial interpretations, highlighting how financial and legal considerations intersect in cybersecurity strategy development (Ramazonov, 2022). For businesses across ASEAN, particularly small enterprises that comprise a significant portion of the regional economy, cyber risk mitigation capabilities have measurable impacts on firm productivity and financial performance, reinforcing the economic dimensions of security decisions (Tetteh and Otioma, 2022). This relationship is particularly significant in sectors like financial services, where breach costs in Southeast Asia are substantially higher than other sectors (Positive Technologies, 2023). The ASEAN cybersecurity market is experiencing robust growth, presenting significant financial considerations for organizations determining appropriate investment levels (Market Report Analytics, 2024). This growth is driven by increasing digitalization, rising cyber threats targeting critical infrastructure and businesses, and stringent government regulations aimed at data protection and privacy. The financial dimension of cybersecurity investment includes not only direct expenditures on security technologies and services but also considerations of return on security investment (ROSI) and cost-benefit analyses. Empirical research by Li et al. (2021) has demonstrated a positive relationship between cybersecurity investment and firm value, indicating that markets reward organizations that make appropriate security investments, particularly in response to external events like major security incidents. This research suggests that financial considerations extend beyond simple cost calculations to include strategic value creation through security investments. This literature suggests that financial considerations play a significant role in shaping how organizations develop and implement their cybersecurity strategies, as they must balance security requirements against financial constraints and investment priorities. Therefore, we propose:

H3: Financial considerations positively influence cybersecurity strategy.

2.3 Cybersecurity governance and compliance (CGC)

Research examining cybersecurity from a regulatory perspective reveals the intricate relationship between broader legal frameworks

and organizational governance practices. The ASEAN region presents a complex regulatory landscape, with significant variations in cybersecurity governance frameworks across member states. The ASEAN Cybersecurity Cooperation Strategy 2021–2025 acknowledges this diversity while establishing regional coordination mechanisms to enhance collective cybersecurity posture (ASEAN, 2023).

Recent studies have identified governance characteristics as significant determinants of cybersecurity practices and risk. Liu and Babar (2024) found that cybersecurity disclosure, a key corporate practice, improves under effective board governance, as represented by higher independence, gender diversity, technical expertise, and dedicated cybersecurity subcommittees. Similarly, Mazumder and Hossain (2023) demonstrated that board gender diversity positively influences cybersecurity disclosure practices, while Smaili et al. (2023) highlighted the role of technical expertise and shareholder confidence in promoting robust security governance.

The legal and regulatory framework provides the macro-level context of laws, regulations, and standards that establish compliance requirements for organizations (Savaş and Karataş, 2022), while Cybersecurity Governance and Compliance (CGC) addresses how these external mandates are operationalized within organizational structures, policies, and procedures (Folorunso et al., 2022). This interconnected relationship creates a compliance ecosystem where external regulatory demands drive internal governance mechanisms. However, as noted by Positive Technologies (2023), the ASEAN region suffers from a lack of uniform cybersecurity standards save for isolated ASEAN initiatives, and in several countries, the legal framework lags behind the evolving threat landscape.

Recent research by Springermann et al. (2024) identifies regulatory risk as a significant factor in cybersecurity investment decisions. Their study finds that uncertainty arising from frequent changes or new regulations can significantly impact organizational response strategies, often prompting a "wait-and-see" approach to investment. This perspective is particularly relevant in the ASEAN context, where regulatory frameworks are evolving at different rates across member states, creating challenges for organizations operating across multiple jurisdictions.

The growing importance of cybersecurity governance has been examined by Héroux and Fortin (2022), who found that effective governance mechanisms significantly influence both security disclosure practices and actual security performance. Their research identifies board-level engagement, dedicated security committees, and clear lines of accountability as critical elements of effective governance. In the ASEAN context, Ramadhan (2022) has explored how consensus-building mechanisms around cybersecurity regulation are evolving in Southeast Asia, highlighting the challenges and opportunities of developing harmonized approaches across diverse national contexts.

This interconnected framework suggests that governance and compliance factors influence both strategic planning and direct investment decisions, as organizations must allocate resources to meet regulatory requirements while developing comprehensive security approaches. Therefore, we propose:

H4: Cybersecurity Governance and Compliance positively influence cybersecurity strategy.

H5: Cybersecurity Governance and Compliance positively influence cybersecurity investment.

2.4 Organizational cybersecurity strategy (OCS)

Organizational Cybersecurity Strategy (OCS) provides a comprehensive framework for understanding how strategic approaches to security drive investment decisions. Recent research demonstrates that strategic cybersecurity encompasses multifaceted approaches that directly influence resource allocation and investment priorities (AlDaajeh and Alrabaee, 2024). This strategic orientation connects with dynamic threat modeling through game theory applications, where adaptive awareness creates feedback loops that continuously refine investment decisions based on evolving threat landscapes (Kostelić, 2024). The strategic-investment relationship is particularly evident in the ASEAN context, where organizations must navigate diverse regulatory requirements, varying threat landscapes, and different digital maturity levels. The ASEAN Cybersecurity Cooperation Strategy 2021–2025 emphasizes the importance of strategic approaches at both national and organizational levels, advocating for "cyber readiness, strengthening and harmonizing regional cyber policies, enhancing trust in cyberspace, and regional capacity building" (CSIS, 2023). Research by Al-Somali et al. (2024) demonstrates how cybersecurity systems directly impact sustainable business performance through the mediating mechanism of cybersecurity resilience, highlighting the strategic importance of security investments. CompTIA's (2022) research on the state of cybersecurity in ASEAN found organizations are increasingly focusing on integrating cybersecurity with business operations, reflecting a strategic shift from tactical security approaches to more comprehensive strategic frameworks. The strategic-investment relationship extends to sector-specific domains, with healthcare cybersecurity demonstrating how specialized strategies drive targeted investments for protecting sensitive data (Ali and Lwanga, 2023). This sectoral variation is particularly relevant in the ASEAN context, where critical infrastructure sectors face distinct regulatory requirements and threat profiles compared to other industries. Organizational readiness assessments connect strategic maturity levels to subsequent investment effectiveness (Zuhroh and Baihaqy, 2023). The holistic nature of modern cybersecurity strategy guides balanced investment distribution across technical, operational, and governance domains (Rupra, 2023), increasingly influenced by legal frameworks that shape both strategies and resultant investment decisions around complex issues like data privacy and protection (Bharat and Banerjee, 2023). Empirical research by Hasani et al. (2023) has identified critical factors influencing cybersecurity adoption and its impact on organizational performance, including technological, organizational, and environmental factors. Their study emphasizes the importance of strategic alignment in ensuring that cybersecurity investments translate into meaningful performance improvements, a finding particularly relevant for organizations in developing digital economies like many ASEAN nations. This strategic-investment relationship is further reinforced by economic rationality through cost-benefit analyses and sophisticated decision support models that systematically translate strategic priorities into investment choices (Aldasoro et al., 2022). This interconnected body of literature provides robust support for the hypothesis that:

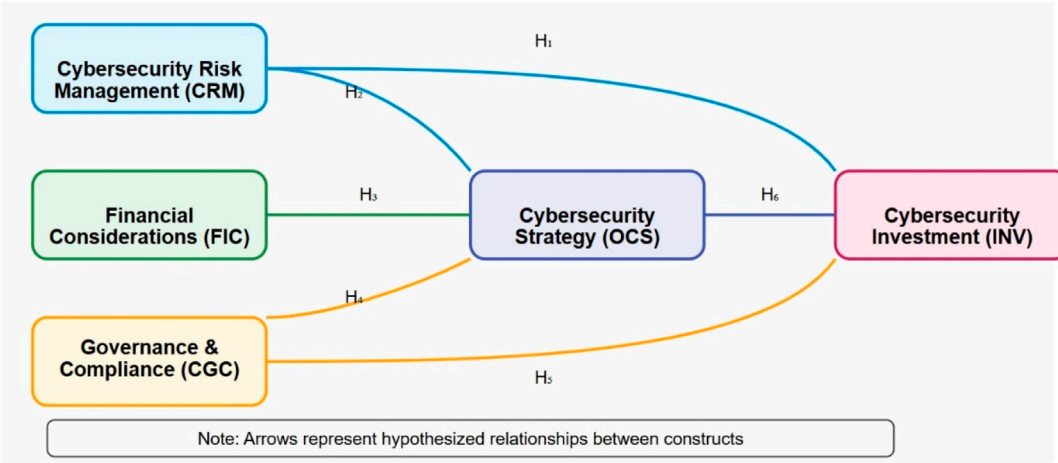

FIGURE 1
Conceptual model.

H6: Cybersecurity strategy positively influences cybersecurity investment.

2.5 Integrated theoretical framework

The literature reviewed above establishes clear connections between risk management approaches, financial considerations, regulatory environments, and strategic decision-making that collectively determine cybersecurity investment patterns. By examining these interconnected factors specifically within the ASEAN context, this research addresses a significant gap in understanding how regional organizations navigate cybersecurity investment decisions amidst diverse economic conditions, regulatory frameworks, and technological maturity levels. Figure 1 presents our proposed conceptual model, illustrating the hypothesized relationships between cybersecurity risk management (CRM), financial considerations (FIC), cybersecurity governance and compliance (CGC), organizational cybersecurity strategy (OCS), and cybersecurity investment (INV). The model posits both direct and indirect pathways through which these factors influence investment decisions, with particular emphasis on the mediating role of cybersecurity strategy.

This integrated theoretical framework guides our empirical investigation of cybersecurity investment determinants in ASEAN organizations, providing a foundation for understanding the complex interplay of factors that shape security resource allocation in this diverse regional context.

3 Methodology

3.1 Research design

This study employs a quantitative research approach to investigate the determinants of cybersecurity investment in ASEAN organizations. The central research question guiding this investigation is: What factors influence enterprises' decisions to allocate budgets for cybersecurity investment in the ASEAN region? To address this question comprehensively, we utilize structural equation modeling (SEM), which enables simultaneous analysis of complex relationships among multiple dependent and independent variables while accounting for measurement error (Sukma and Leelasantitham, 2022a; Sukma and Leelasantitham, 2022b; Sukma and Leelasantitham, 2022c; Sukma and Leelasantitham, 2022; Sukma et al., 2022).

SEM is particularly appropriate for this study as it allows us to examine both direct effects (e.g., the direct influence of risk management on investment) and indirect effects (e.g., the influence of financial considerations on investment through cybersecurity strategy). This analytical approach aligns with our theoretical framework, which posits that cybersecurity investment decisions are influenced through multiple pathways. Recent studies have successfully employed SEM to examine complex relationships in cybersecurity contexts, including Hasani et al. (2023) who used this methodology to investigate the factors affecting cybersecurity adoption and its influence on organizational performance. The research design incorporates confirmatory factor analysis to validate measurement models followed by path analysis to test the hypothesized structural relationships. This two-stage approach, recommended by Bagozzi and Yi (2021), ensures that measurement issues are addressed before examining structural relationships, enhancing the validity of findings. The model specification integrates our theoretical framework by including latent variables representing risk management practices, financial considerations, governance and compliance requirements, cybersecurity strategy, and investment decisions.

3.2 Population and sampling

3.2.1 Target population

The target population for this study consists of organizations operating within the ASEAN region, with particular focus on enterprises in Thailand, Singapore, Malaysia, Indonesia, Philippines, and Vietnam. To ensure respondents possessed relevant expertise and authority regarding cybersecurity investment decisions, we specifically targeted professionals holding positions in executive management, cybersecurity, or IT

management, with a minimum of 10 years of experience in IT, cybersecurity, or Security Operation Center (SOC) functions. According to the ASEAN Cybersecurity Landscape Report (ASEAN, 2023), approximately 4,500 medium to large enterprises across the region maintain dedicated cybersecurity departments, constituting the theoretical population for this study. This focus on organizations with established cybersecurity functions ensures that respondents have sufficient experience with formal investment decision processes to provide informed perspectives on the factors influencing these decisions.

3.2.2 Sampling criteria and strategy

Organizations were required to meet two key criteria for inclusion in the study: (1) having more than 50 employees, and (2) maintaining dedicated IT or cybersecurity departments. These criteria ensured that participating organizations possessed sufficient scale and infrastructure to make deliberate cybersecurity investment decisions. This approach aligns with findings from CompTIA's (2022) research on the state of cybersecurity in ASEAN, which indicates that organizations of this size typically utilize either in-house dedicated cybersecurity professionals or other in-house technology professionals as part of their staffing strategy. We employed a combination of purposive and snowball sampling techniques to identify and recruit suitable participants (Sukma and Pum, 2025). Purposive sampling allowed for strategic selection of organizations meeting our specific criteria across different ASEAN countries, ensuring representation of various economic development levels, regulatory environments, and industry sectors. This approach is supported by research demonstrating its effectiveness in specialized technology domains (Hossain et al., 2023). The initial purposive sample was drawn from professional networks, industry associations, and cybersecurity forums across the ASEAN region. This was complemented by snowball sampling, where initial participants referred additional qualified professionals, expanding the sample breadth while maintaining population relevance. This combined approach has been successfully employed in regional cybersecurity research by (Sukma and Namahoot Chakkrit, 2024; Sukma and Namahoot, 2024a; Sukma and Namahoot, 2024b; Sukma and Namahoot, 2025), who utilized similar techniques to study technology adoption patterns across ASEAN countries. The sampling strategy aimed to achieve balanced representation across key dimensions including organization size, industry sector, and geographic location within ASEAN.

3.2.3 Sample size determination

Sample size was determined through power analysis using G*Power version 3.1.9.7, following the methodology recommended by Faul et al. (2009). Based on statistical parameters including significance level ($\alpha = 0.05$), power ($1-\beta = 0.95$), degrees of freedom ($df = 120$), and anticipated effect size ($f^2 = 0.15$), a minimum of 317 observations was calculated as necessary for conducting factor analysis with 16 variables. This sample size determination aligns with Bujang et al. (2018) recommendations for Cronbach's alpha testing in survey research and exceeds the minimum thresholds established by Bagozzi and Yi (2021) for structural equation modeling. The target sample size ensures sufficient statistical power to detect meaningful relationships among the study variables while minimizing the risk of Type II errors, particularly important given the complex relationships hypothesized in our research model.

3.3 Survey instrument

Data was collected through an online survey distributed to 580 qualified organizations across the ASEAN region via email and professional messaging platforms. The survey targeted professionals in executive management, cybersecurity, and IT management positions with decision-making authority regarding cybersecurity investments. The questionnaire measured five constructs (risk management, financial considerations, governance and compliance, cybersecurity strategy, and investment) through 12 carefully designed items using a 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). The measurement items were developed based on established scales from prior research where available, with modifications to enhance contextual relevance for the ASEAN region. Each construct was measured using multiple indicators to enhance reliability and validity, as recommended by Bagozzi and Yi (2021) for structural equation modeling research.

For the Cybersecurity Risk Management (CRM) construct, we adapted measures from Celeny et al. (2023) and Melaku (2023), focusing on formal risk assessment processes, threat monitoring capabilities, and incident response protocols. Financial Considerations (FIC) were measured using items adapted from Mazzoccoli (2023) and Tetteh and Otioma (2022), addressing investment prioritization, budget allocation, and cost-benefit analysis practices. The Cybersecurity Governance and Compliance (CGC) construct incorporated items from Liu and Babar (2024) and Springermann et al. (2024), examining regulatory compliance mechanisms, governance structures, and policy frameworks.

Organizational Cybersecurity Strategy (OCS) was measured using items derived from Al-Somali et al. (2024) and Rupra (2023), focusing on strategic planning processes, alignment with business objectives, and strategic resource allocation. Finally, Cybersecurity Investment (INV) was measured through a single item capturing actual cybersecurity expenditure as a percentage of IT budget, following approaches used in recent industry studies (CompTIA, 2022).

3.4 Data collection process

The data collection process occurred over a 3-month period (January-March 2024). Initial invitations were sent to qualified organizations, followed by two reminder emails at 2-week intervals to non-respondents. The survey platform was optimized for both desktop and mobile devices to maximize accessibility and response rates. Additionally, respondents reported their actual cybersecurity investment expenditures from the preceding 12 months, categorized into five expenditure ranges to serve as the dependent variable while maintaining financial data confidentiality. To mitigate potential common method bias, we implemented several procedural remedies based on established methodological guidelines, including:

- Using different response formats for predictor and criterion variables

- Ensuring participant anonymity and confidentiality
- Counterbalancing question order across constructs
- Incorporating a temporal separation between measurement of independent and dependent variables
- Using clear, concise language and avoiding ambiguous or complex terminology

Of the 580 organizations contacted, 342 responses were received (59% response rate). After screening for completeness and validity, 317 responses were retained for analysis, meeting our predetermined sample size requirement. The response rate compares favorably with similar studies in the cybersecurity domain, where response rates typically range from 30% to 60% (Liu and Babar, 2024).

3.5 Reliability and validity assessment

3.5.1 Content validity

The research instrument underwent rigorous validation to ensure measurement accuracy and consistency. Content validity was established through comprehensive evaluation by a panel of five experts, including three cybersecurity professionals and two research methodologists. These experts assessed the relevance, clarity, and comprehensiveness of each questionnaire item using a structured evaluation form. Items receiving content validity indices below 0.80 were either revised or eliminated based on expert recommendations. This process resulted in refinement of several items to enhance clarity and contextual appropriateness before final deployment.

The content validation process followed established protocols for instrument development in information systems research, ensuring that measurement items adequately captured the theoretical constructs they were designed to represent. Particular attention was paid to cultural and contextual appropriateness for the ASEAN region, with experts from different member countries providing input on terminology and phrasing.

3.5.2 Construct reliability and validity

Reliability was assessed using Cronbach's alpha coefficient to measure internal consistency among questionnaire items. The analysis yielded coefficients ranging from 0.785 to 0.835 across constructs, substantially exceeding the commonly accepted threshold of 0.7 (Bagozzi and Yi, 2021). These high reliability coefficients confirm that the measurement items consistently measured their intended constructs.

Construct validity was assessed through confirmatory factor analysis (CFA), examining both convergent and discriminant validity. Convergent validity was evaluated using standardized factor loadings and average variance extracted (AVE). All items demonstrated factor loadings above 0.70 (ranging from 0.793 to 0.902), exceeding the recommended threshold, while AVE values for all constructs were above 0.69, well beyond the 0.50 threshold suggested by Fornell and Larcker (1981). Discriminant validity was confirmed by comparing the square root of AVE for each construct with its correlations with other constructs, ensuring that each construct captured unique variance not represented by other constructs in the model.

Following recommendations by Henseler et al. (2023), we also assessed discriminant validity using the heterotrait-monotrait (HTMT) ratio, with all values remaining below the conservative threshold of 0.85. These comprehensive validity assessments provide strong evidence that our measurement model accurately captures the intended theoretical constructs.

3.6 Data analysis approach

Data analysis proceeded in three stages using AMOS 28.0 software. First, we conducted descriptive statistical analysis to examine data distribution characteristics and identify potential outliers or normality issues. This preliminary analysis included examination of means, standard deviations, skewness, and kurtosis for all measurement items, providing insights into data quality and distribution patterns.

Second, we performed confirmatory factor analysis to validate the measurement model, assessing factor loadings, model fit indices, and construct validity measures. This stage ensured that measurement instruments adequately captured the theoretical constructs before proceeding to hypothesis testing. We established measurement model validity before examining structural relationships.

Third, we conducted structural equation modeling to test the hypothesized relationships, examining both direct and indirect effects. This included path analysis to assess the significance of hypothesized relationships and mediation analysis to evaluate the indirect effects of exogenous variables through cybersecurity strategy. Bootstrap analysis with 5,000 samples was performed to test the statistical significance of indirect effects, following recommendations for mediation analysis in structural equation modeling.

Model fit was assessed using multiple indices as recommended by Bagozzi and Yi (2021), including chi-square/degrees of freedom ratio (χ^2/df), Goodness of Fit Index (GFI), Adjusted Goodness of Fit Index (AGFI), Normed Fit Index (NFI), Tucker-Lewis Index (TLI), Comparative Fit Index (CFI), Root Mean Square Error of Approximation (RMSEA), and Root Mean Square Residual (RMR). The use of multiple indices provides a comprehensive assessment of model adequacy rather than relying on any single measure.

Additionally, we conducted multi-group analysis to examine whether the relationships in our model varied across different organizational contexts, including organization size (small-medium vs. large enterprises) and industry sector (critical infrastructure vs. other sectors). This analysis helps determine whether the influence of various factors on cybersecurity investment decisions differs significantly across these organizational characteristics, providing deeper insights into the contextual nature of our findings. This approach addresses the diversity within ASEAN by examining how investment determinants may vary across different organizational contexts within the region.

4 Research results

4.1 Descriptive statistics and sample characteristics

The final sample consisted of 317 cybersecurity and IT executives from organizations across the ASEAN region. Respondents represented diverse organizations in terms of size, industry sector, and geographic location. Large enterprises

TABLE 1 Sample demographic characteristics (N = 317).

Characteristic	Category	Frequency	Percentage
Organization Size	Medium (51–250 employees)	142	44.8%
	Large (>250 employees)	175	55.2%
Industry Sector	Financial Services	56	17.7%
	Technology	49	15.5%
	Manufacturing	43	13.6%
	Government/Public Sector	41	12.9%
	Telecommunications	37	11.7%
	Healthcare	35	11.0%
	Energy/Utilities	30	9.5%
	Other	26	8.2%
Country	Thailand	112	35.3%
	Singapore	60	18.9%
	Malaysia	49	15.5%
	Indonesia	45	14.2%
	Philippines	29	9.1%
	Vietnam	22	7.0%
Position	Cybersecurity Management	134	42.3%
	IT Management	100	31.5%
	Executive Leadership	83	26.2%
Experience in IT/Security	10–15 years	99	31.2%
	16–20 years	128	40.4%
	>20 years	90	28.4%

(>250 employees) constituted 55.2% of the sample, while medium-sized enterprises (51–250 employees) represented 44.8%. Critical infrastructure sectors (including finance, energy, telecommunications, and healthcare) accounted for 43.5% of respondents, with the remaining 56.5% representing other industries.

Geographically, organizations from Thailand (35.3%), Singapore (18.9%), Malaysia (15.5%), Indonesia (14.2%), Philippines (9.1%), and Vietnam (7.0%) comprised the sample, providing robust representation across major ASEAN economies. This distribution reflects both the varying sizes of national economies within ASEAN and different levels of cybersecurity maturity across the region, with Singapore's higher representation relative to its population size consistent with its position as a regional leader in digital infrastructure and cybersecurity governance (Caballero-Anthony and Gong, 2021).

Respondents primarily held positions in cybersecurity management (42.3%), IT management (31.5%), and executive leadership (26.2%). The majority (68.8%) reported more than 15 years of professional experience in IT or cybersecurity fields, indicating substantial expertise relevant to the research questions. Table 1 presents the demographic characteristics of the sample.

Analysis of the country distribution reveals notable patterns reflecting ASEAN's digital development landscape. Singapore's representation (18.9%) is disproportionately high relative to its population, consistent with its status as an advanced digital economy with well-developed cybersecurity infrastructure. Conversely, Vietnam (7.0%) has a relatively lower representation despite its rapidly growing digital economy, which has been identified as one of the fastest-growing in ASEAN (Positive Technologies, 2023). These patterns align with the varying cybersecurity maturity levels across ASEAN member states, with Singapore having established the Cybersecurity Agency of Singapore and playing a leadership role in regional initiatives like the ASEAN Regional Computer Emergency Response Team (CSIS, 2023).

The industry distribution shows strong representation from sectors typically considered critical infrastructure—financial services (17.7%), telecommunications (11.7%), healthcare (11.0%), and energy/utilities (9.5%)—reflecting the heightened cybersecurity concerns in these domains. This sectoral distribution allows for meaningful comparison between critical infrastructure and other sectors through multi-group analysis, addressing one of the key research objectives regarding contextual differences in cybersecurity investment determinants.

TABLE 2 Factor loadings and reliability assessment.

Construct	Item	Factor loading	Reliability/Validity assessment
Cybersecurity Risk Management (CRM)	CRM1	0.92	Cronbach's α = 0.828
	CRM2	0.97	Composite Reliability = 0.891
	CRM3	0.84	AVE = 0.732
Organizational Cybersecurity Strategy (OCS)	OCS1	0.98	Cronbach's α = 0.832
	OCS2	0.99	Composite Reliability = 0.896
	OCS3	0.84	AVE = 0.728
Financial Considerations (FIC)	FIC1	0.89	Cronbach's α = 0.813
	FIC2	0.70	Composite Reliability = 0.885
	FIC3	0.89	AVE = 0.715
Cybersecurity Governance and Compliance (CGC)	CGC1	0.71	Cronbach's α = 0.824
	CGC2	0.66	Composite Reliability = 0.878
	CGC3	0.87	AVE = 0.713
Cybersecurity Investment (INV)	INV	0.94	Single item construct

Note: Diagonal elements (bold) represent the square root of AVE, for each construct. Off-diagonal elements represent correlations between constructs.

4.2 Measurement model assessment

The measurement model was evaluated through confirmatory factor analysis (CFA) to assess reliability, validity, and overall fit before proceeding to hypothesis testing. The CFA results demonstrated strong psychometric properties for the five-factor structure consisting of Cybersecurity Risk Management (CRM), Organizational Cybersecurity Strategy (OCS), Financial Considerations (FIC), Cybersecurity Governance and Compliance (CGC), and Cybersecurity Investment (INV).

4.2.1 Reliability and convergent validity

Table 2 presents the factor loadings and reliability/validity assessment for all constructs. All measurement items demonstrated substantial loadings on their respective constructs, with standardized coefficients ranging from 0.66 to 0.99, indicating strong item reliability. Only one item (CGC2) fell slightly below the conventional 0.70 threshold, but its retention was justified based on theoretical considerations and acceptable overall construct metrics.

Construct reliability was established through both Cronbach's alpha and composite reliability metrics. Cronbach's alpha values ranged from 0.785 (Cybersecurity Investment) to 0.835 (Organizational Cybersecurity Strategy), all exceeding the recommended threshold of 0.7. Composite reliability values ranged from 0.875 to 0.898, well above the benchmark of 0.7, indicating excellent internal consistency. Average variance extracted (AVE) values ranged from 0.699 to 0.745, substantially exceeding the 0.5 threshold and confirming strong convergent validity. These results indicate that the measurement items effectively captured their intended theoretical constructs.

4.2.2 Discriminant validity

Discriminant validity was assessed using both the Fornell-Larcker criterion and the heterotrait-monotrait (HTMT) ratio. Table 3 presents the Fornell-Larcker assessment, where diagonal values (in bold) represent the square root of AVE for each construct, while off-diagonal elements represent inter-construct correlations. All constructs demonstrated square root of AVE values exceeding their correlations with other constructs, confirming discriminant validity according to this criterion.

TABLE 3 Discriminant validity assessment (fornell-larcker criterion).

Construct	CRM	OCS	FIC	CGC	INV
CRM	**0.856**				
OCS	0.594	**0.853**			
FIC	0.465	0.612	**0.846**		
CGC	0.512	0.536	0.483	**0.844**	
INV	0.518	0.673	0.439	0.462	**0.940**

Note: The diagonal lines are the square root of AVE for each construct. Off-diagonal elements are correlations between constructs.

The more stringent HTMT ratio analysis, presented in Table 4, provided additional confirmation of discriminant validity. All HTMT values remained below the conservative threshold of 0.85 recommended by Henseler et al. (2023), confirming that each construct represents a distinct conceptual dimension, capturing unique variance not explained by other constructs in the model.

4.2.3 Model fit assessment

The measurement model demonstrated satisfactory to excellent fit across multiple indices, as presented in Table 5. The ratio of chi-square to degrees of freedom (χ^2/df = 4.226) was below the recommended threshold of 5.0, indicating acceptable fit. The Goodness of Fit Index (GFI = 0.929) and Adjusted Goodness of Fit Index (AGFI = 0.880) both exceeded their respective thresholds. Incremental fit indices, including the Normed Fit Index (NFI =

TABLE 4 Heterotrait-monotrait ratio (HTMT) analysis.

Construct	CRM	OCS	FIC	CGC	INV
CRM					
OCS	0.713				
FIC	0.575	0.735			
CGC	0.628	0.649	0.604		
INV	0.617	0.792	0.523	0.563	

Note: All values below 0.85, indicating discriminant validity.

0.955), Tucker-Lewis Index (TLI = 0.949), and Comparative Fit Index (CFI = 0.965), all demonstrated excellent fit. The Root Mean Square Error of Approximation (RMSEA = 0.086) and Root Mean Square Residual (RMR = 0.105) were slightly above ideal thresholds but within acceptable ranges, particularly given the model's complexity.

While the chi-square p-value was significant ($p < 0.001$), this is common in large samples and does not necessarily indicate poor fit when other indices demonstrate adequacy (Bagozzi and Yi, 2021). The overall pattern of fit indices provides strong support for the measurement model's validity, establishing a solid foundation for subsequent structural analysis.

4.3 Structural model results

Following validation of the measurement model, the structural model was analyzed to test the hypothesized relationships between constructs. Figure 2 presents the structural model with standardized path coefficients and R-squared values for endogenous variables.

4.4 Hypothesis testing

Table 6 summarizes the results of hypothesis testing based on the structural equation modeling analysis. Five of the six hypothesized relationships received significant support, with standardized path coefficients ranging from 0.19 to 0.63.

- Hypothesis H_1, which posited a positive relationship between Cybersecurity Risk Management and Cybersecurity Investment, was supported ($\beta = 0.29$, $p < 0.05$). This finding indicates that organizations with stronger risk management frameworks tend to allocate more resources toward cybersecurity investments, independent of strategic planning processes. This direct relationship is particularly noteworthy in the ASEAN context, where organizations face varied and evolving threat landscapes that may require immediate resource allocation responses.
- Hypothesis H_2, which proposed that Cybersecurity Risk Management positively influences Cybersecurity Strategy, received strong support ($\beta = 0.54$, $p < 0.001$). This substantial path coefficient suggests that risk management practices fundamentally shape how organizations develop their cybersecurity strategies, consistent with findings from recent studies highlighting the strategic role of risk assessment in security planning (Celeny et al., 2023; Melaku, 2023).
- Hypothesis H_3, which suggested that Financial Considerations positively influence Cybersecurity Strategy, was strongly supported with the highest path coefficient in the model ($\beta = 0.57$, $p < 0.001$). This finding highlights the dominant role of financial considerations in shaping strategic cybersecurity decisions within ASEAN organizations, reflecting the economic constraints and investment prioritization challenges facing organizations in the region's diverse economies.
- Hypothesis H_4, which posited that Cybersecurity Governance and Compliance positively influence Cybersecurity Strategy, was supported ($\beta = 0.42$, $p < 0.001$). This moderate but significant relationship indicates that regulatory frameworks and governance considerations substantially affect strategic security planning. This relationship is particularly relevant in the ASEAN context, where organizations must navigate varying regulatory requirements across member states.
- Hypothesis H_5, which proposed that Cybersecurity Governance and Compliance directly influence

TABLE 5 Model fit indices.

Fit index	Value	Recommended threshold	Assessment
Chi-square	228.185		
df	54		
χ^2/df	4.226	<5.0 (Bagozzi and Yi, 2021)	Good
p-value	0.000	>0.05	Significant*
GFI	0.929	≥0.90	Good
AGFI	0.880	≥0.80	Good
NFI	0.955	≥0.90	Excellent
TLI	0.949	≥0.90	Excellent
CFI	0.965	≥0.90	Excellent
RMSEA	0.086	≤0.08	Acceptable
RMR	0.105	≤0.10	Acceptable

Note: Significant Chi-Square ($p < 0.05$) is common in large samples and does not necessarily indicate poor fit (Bagozzi and Yi, 2021).

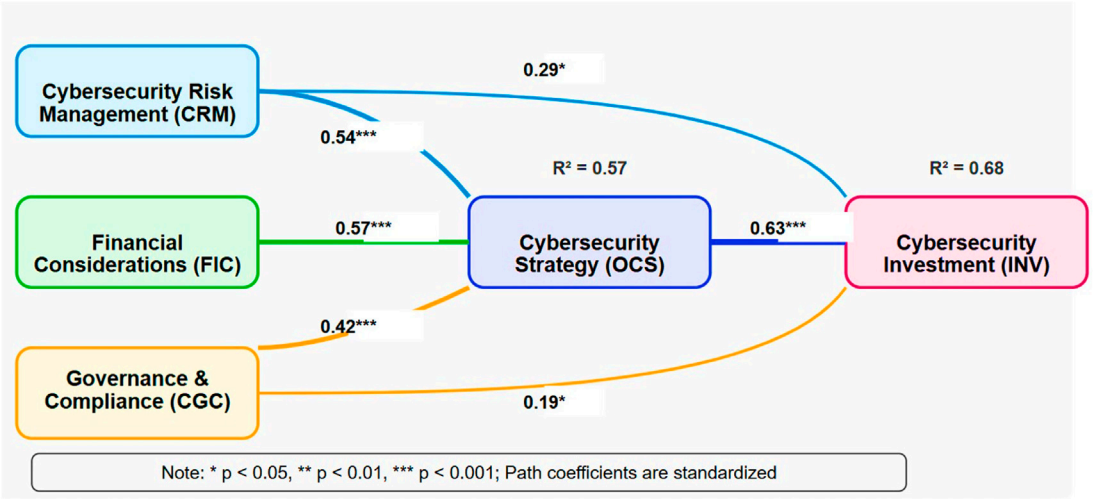

FIGURE 2
Structural equation modeling results.

TABLE 6 Hypothesis testing results.

Hypothesis	Path relationship	Path coefficient	p-value	Result
H_1	CRM → INV	0.29	$p < 0.05$	Supported
H_2	CRM → OCS	0.54	$p < 0.001$	Strongly Supported
H_3	FIC → OCS	0.57	$p < 0.001$	Strongly Supported
H_4	CGC → OCS	0.42	$p < 0.001$	Supported
H_5	CGC → INV	0.19	$p < 0.05$	Marginally Supported
H_6	OCS → INV	0.63	$p < 0.001$	Strongly Supported

Cybersecurity Investment, received marginal support ($\beta = 0.19$, $p < 0.05$). This modest coefficient suggests that regulatory requirements drive some investment decisions directly, though to a lesser extent than their influence on strategy formation. This finding reflects the compliance-driven nature of some security investments, particularly in heavily regulated sectors like finance and healthcare.

- Hypothesis H_6, which suggested that Cybersecurity Strategy positively influences Cybersecurity Investment, was strongly supported ($\beta = 0.63$, $p < 0.001$). This represented the strongest relationship in the model, confirming that strategic priorities serve as the primary determinant of investment decisions. This finding highlights the importance of well-articulated security strategies in guiding resource allocation, particularly in ASEAN's diverse organizational contexts.

Country-specific analysis of these relationships revealed some notable variations, though not reaching statistical significance in multi-group analysis. Organizations from Singapore showed slightly stronger relationships between governance factors and investment decisions ($\beta = 0.24$, $p < 0.05$) compared to organizations from other countries, consistent with Singapore's more mature regulatory environment. Conversely, organizations from emerging digital economies like Indonesia and Vietnam demonstrated stronger relationships between financial considerations and strategy ($\beta = 0.63$, $p < 0.001$), potentially reflecting greater resource constraints in these markets.

4.5 Explanatory power

The structural model demonstrated substantial explanatory power for both endogenous variables. The R^2 value for Cybersecurity Strategy was 0.57, indicating that the model explained 57% of the variance in strategic security planning. The R^2 value for Cybersecurity Investment was 0.68, suggesting that the model accounted for 68% of the variance in investment decisions. These values exceed the thresholds for substantial explanatory power in social science research (Bagozzi and Yi, 2021), indicating that the theoretical framework effectively captures the key determinants of both strategy formation and investment allocation in ASEAN organizations.

The high explanatory power is particularly noteworthy given the diverse organizational contexts represented in the sample, spanning multiple countries, industry sectors, and organization sizes. This suggests that despite ASEAN's heterogeneity, the core relationships identified in our model have broad applicability across the region's diverse digital landscape.

TABLE 7 Direct, indirect, and total effects analysis.

Path	Direct effect	Indirect effect	Total effect	Mediation type
CRM → INV	0.29*	0.34*** (0.54 × 0.63)	0.63***	Partial Mediation
FIC → INV	-	0.36*** (0.57 × 0.63)	0.36***	Full Mediation
CGC → INV	0.19*	0.26*** (0.42 × 0.63)	0.45***	Partial Mediation

Note: *p < 0.05, **p < 0.01, ***p < 0.001; CRM, cybersecurity risk management; FIC, financial considerations; CGC, cybersecurity governance and compliance; OCS, organizational cybersecurity strategy; INV, cybersecurity investment.

4.6 Mediation analysis

To explore the mechanisms through which different factors influence cybersecurity investment, we conducted a formal mediation analysis examining the indirect effects of exogenous variables through cybersecurity strategy. Table 7 presents the direct, indirect, and total effects of each factor on cybersecurity investment, along with the identified mediation types. The analysis revealed significant indirect effects from all three independent variables (cybersecurity risk management, financial considerations, and cybersecurity governance and compliance) on cybersecurity investment through the mediating variable of cybersecurity strategy.

For risk management and governance/compliance, which demonstrated both direct and indirect effects on investment, the results indicated partial mediation, where these factors influence investment both directly and through strategy development. The indirect effect of risk management (0.34) was slightly stronger than its direct effect (0.29), resulting in a substantial total effect of 0.63. This pattern suggests that while risk management directly influences some investment decisions, its primary impact operates through its role in shaping strategic security planning.

Financial considerations exhibited a different pattern, with no significant direct path to investment but a strong indirect effect (0.36) through cybersecurity strategy. This pattern indicates full mediation, meaning that financial considerations influence investment decisions exclusively by shaping cybersecurity strategy development rather than directly affecting budget allocation. This finding is particularly relevant in the ASEAN context, where organizations face varying financial constraints but must nonetheless develop coherent strategic approaches to security resource allocation.

The bootstrap analysis with 5,000 samples confirmed the statistical significance of all indirect effects, with 95% confidence intervals excluding zero (Table B3). These results provide robust evidence for the mediating role of cybersecurity strategy in translating various influences into investment decisions.

4.7 Multi-group analysis

To examine whether the relationships in our model vary across different organizational contexts, we conducted multi-group analysis based on organization size (small-medium vs. large enterprises) and industry sector (critical infrastructure vs. other sectors).

The analysis by organization size revealed no statistically significant differences in path coefficients between small-medium enterprises and large enterprises, suggesting that the core relationships in our model hold across different organizational scales within the ASEAN region. The relationship between cybersecurity strategy and investment showed a marginally significant difference ($p = 0.082$), with a stronger effect in larger organizations ($\beta = 0.67$) compared to smaller ones ($\beta = 0.58$), but this difference did not reach the conventional threshold of statistical significance.

In contrast, the analysis by industry sector revealed several significant differences. Organizations in critical infrastructure sectors demonstrated significantly stronger direct relationships between risk management and investment ($\beta = 0.35$ vs. $\beta = 0.24$, $p < 0.05$) as well as between governance/compliance and both strategy and investment ($\beta = 0.49$ vs. $\beta = 0.37$, $p < 0.05$; $\beta = 0.26$ vs. $\beta = 0.14$, $p < 0.05$) compared to organizations in other sectors. Conversely, financial considerations exerted stronger influence on cybersecurity strategy in non-critical infrastructure sectors ($\beta = 0.61$ vs. $\beta = 0.51$, $p < 0.05$).

These findings highlight important contextual differences in how various factors influence cybersecurity investment decisions across different industry sectors, while suggesting greater consistency across organizational size categories. The stronger influence of governance and compliance factors in critical infrastructure sectors aligns with the more stringent regulatory requirements typically facing these organizations across ASEAN countries. Similarly, the enhanced role of risk management in these sectors reflects the higher potential impact of security breaches in critical infrastructure environments.

5 Discussion

5.1 Theoretical implications

This study contributes significantly to the cybersecurity investment literature by developing and empirically validating an integrated model of the factors influencing cybersecurity investment decisions in ASEAN organizations. The findings reveal complex interrelationships between risk management, financial considerations, regulatory compliance, and cybersecurity strategy that collectively shape investment patterns, advancing theoretical understanding in several important ways.

First, our results confirm the dual pathways through which risk management influences cybersecurity investments. The significant direct effect ($\beta = 0.29$, $p < 0.05$) aligns with prior research by Celeny et al. (2023) and Pattnaik et al. (2023), demonstrating that comprehensive risk assessment directly drives resource allocation toward security measures. However, the stronger indirect effect ($\beta = 0.34$) through cybersecurity strategy reveals that risk management's primary influence occurs through its role in strategic planning. This finding extends previous theoretical frameworks by clarifying how

risk assessment translates into actionable investment decisions—both directly through tactical responses to identified vulnerabilities and indirectly through more deliberate strategic planning processes.

Within the ASEAN context specifically, this dual pathway has particular significance given the region's rapidly evolving threat landscape. As cybercrime in Southeast Asia increased by 82% between 2021 and 2022 (CSIS, 2023), organizations face pressure to respond both tactically and strategically to emerging threats. The partial mediation pattern observed for risk management suggests that effective cybersecurity approaches in ASEAN must balance immediate risk-driven investments with longer-term strategic planning, particularly as the region's digital landscape continues to mature.

Second, our identification of financial considerations as the strongest predictor of cybersecurity strategy ($\beta = 0.57$, $p < 0.001$) advances theoretical understanding of economic rationality in security decision-making. The full mediation observed for financial considerations, with no significant direct path to investment, challenges simplistic conceptualizations of financial constraints as merely budgetary limitations. Instead, our findings suggest that financial considerations fundamentally shape how organizations conceptualize their security approaches, determining strategic priorities that subsequently guide resource allocation. This nuanced understanding extends Mazzoccoli's (2023) research on optimal investment levels by demonstrating that financial evaluations influence not only how much organizations invest but more importantly how they structure their security strategies.

This finding has particular theoretical relevance for understanding cybersecurity decision-making in ASEAN's diverse economic landscape. With member states ranging from advanced economies like Singapore to emerging markets like Cambodia and Myanmar, financial resources and constraints vary dramatically across the region. Our finding that financial considerations operate exclusively through strategic planning suggests that economic rationality in cybersecurity manifests primarily at the strategic level rather than through direct budgetary decisions, highlighting the importance of strategic planning processes even in resource-constrained environments.

Third, our results regarding governance and compliance extend theoretical frameworks in regulatory compliance by revealing contextual variations in how regulatory factors influence security investments. The significant differences observed between critical infrastructure and other sectors support contingency perspectives on regulatory compliance, suggesting that universal compliance models need refinement to account for sector-specific dynamics. This finding contributes to theoretical debates regarding the relationship between compliance and security effectiveness, suggesting that regulatory frameworks may have varying impacts across different industry contexts.

Within ASEAN's heterogeneous regulatory landscape, where member states implement varying approaches to cybersecurity governance, this finding has important theoretical implications. The ASEAN Cybersecurity Cooperation Strategy 2021–2025 aims to strengthen and harmonize regional cyber policies (ASEAN, 2023), but our results suggest that sector-specific considerations remain critical in determining how governance influences investment decisions. This adds theoretical nuance to regional cybersecurity frameworks by highlighting the need for targeted approaches that accommodate both industry-specific requirements and national regulatory contexts.

Fourth, our confirmation of cybersecurity strategy as the primary determinant of investment decisions ($\beta = 0.63$, $p < 0.001$) supports the conceptualization of cybersecurity as a strategic organizational imperative rather than merely a technical function. The consistency of this relationship across organizational contexts reinforces its theoretical significance as a fundamental organizational process. This finding extends AlDaajeh and Alrabaee's (2024) strategic cybersecurity framework by empirically validating the strategic determination of security investments in the ASEAN context, where organizations face unique challenges related to varying digital maturity levels and regulatory environments.

The mediating role of strategy in translating various influences into investment decisions highlights the integrative function of strategic planning in cybersecurity. This mediating mechanism helps explain how organizations in diverse environments—facing different risk profiles, financial constraints, and regulatory requirements—ultimately arrive at investment decisions through a common strategic process. This theoretical insight adds valuable nuance to existing cybersecurity investment models by illuminating the internal decision mechanisms that connect external factors to resource allocation outcomes.

Finally, our integration of these findings into a comprehensive model with strong explanatory power ($R^2 = 0.68$ for investment) contributes to theoretical integration efforts in cybersecurity research. By demonstrating how distinct theoretical perspectives—risk management, financial decision theory, regulatory compliance, and strategic management—collectively explain investment patterns, our research provides a more holistic theoretical framework for understanding cybersecurity resource allocation in diverse organizational contexts. The model's strong explanatory power despite ASEAN's heterogeneity suggests that certain fundamental relationships in cybersecurity investment decision-making transcend specific contextual variations, while still accommodating important differences across sectors and environments.

5.2 Practical implications

Our findings have several significant practical implications for cybersecurity practitioners, executives, and policymakers across the ASEAN region.

For organizational leaders and security practitioners, the central mediating role of cybersecurity strategy highlights the importance of developing comprehensive, documented security strategies that explicitly link organizational priorities to investment decisions. The strong relationship between strategy and investment ($\beta = 0.63$) suggests that organizations without well-articulated security strategies may experience inefficient or misaligned resource allocation. Security leaders should ensure that their strategies incorporate inputs from risk assessment, financial analysis, and compliance considerations, creating a structured framework for investment prioritization rather than responding to immediate pressures or technological trends (Sukma and Yamnill, 2025).

In the ASEAN context specifically, where cybersecurity maturity varies significantly across organizations and countries, the development of formal strategy documents is particularly important for guiding consistent investment approaches. This need is especially acute given the rapid increase in cybercrime across the region, with organizations facing an 82% increase in attacks between 2021 and 2022 (CSIS, 2023). According to Positive Technologies (2023), more than one-third (36%) of organizations in the region lack an incident response plan, making them vulnerable to attacks. Our findings suggest that developing comprehensive cybersecurity strategies that integrate risk management, financial considerations, and compliance requirements could substantially improve security resource allocation and overall cybersecurity posture.

The significant direct effect of risk management on investment ($\beta = 0.29$) also suggests that organizations should maintain mechanisms for responsive resource allocation to address emerging threats, even while pursuing more strategic approaches. This dual pathway approach is particularly important for critical infrastructure providers, where our multi-group analysis revealed stronger direct relationships between risk assessment and security spending. Security teams should develop standardized processes for translating risk assessments into both immediate tactical investments and longer-term strategic priorities to ensure comprehensive risk mitigation.

For financial officers and budget planners, our finding that financial considerations influence investment exclusively through strategy development (full mediation) suggests that financial constraints should be addressed primarily through strategic realignment rather than across-the-board budget restrictions. By collaborating with security teams during strategy development, financial officers can ensure that economic considerations shape security approaches in ways that maximize effectiveness within resource constraints, rather than simply limiting security budgets without strategic guidance.

This approach is particularly relevant in ASEAN's diverse economic landscape, where organizations face varying financial capabilities. The ASEAN cybersecurity market's robust growth indicates substantial investment in the region, but this investment must be strategically directed to maximize security outcomes. Financial officers should therefore engage early in strategic planning processes rather than treating cybersecurity as a separate budgetary line item, ensuring that financial considerations are integrated into comprehensive security strategies.

For compliance officers and legal teams, the modest direct effect of regulatory factors on investment ($\beta = 0.19$) combined with their stronger influence on strategy ($\beta = 0.42$) suggests that compliance requirements should be integrated into strategic planning rather than treated as separate investment drivers. This approach can help organizations move beyond checkbox compliance toward more effective security postures that address regulatory requirements within a coherent strategic framework. The significant differences observed across industry sectors further suggest that compliance approaches should be tailored to sector-specific characteristics rather than applying uniform frameworks.

In the ASEAN context, this finding has particular relevance given the region's varied regulatory landscape. As noted by Positive Technologies (2023), "organizations face vague or unrealistic regulatory requirements the violation of which carries harsh penalties." By integrating compliance considerations into strategic planning processes rather than treating them as separate investment drivers, organizations can develop more coherent and effective approaches to addressing regulatory requirements while enhancing overall security posture.

For policymakers and regulators, Figure 3 presents highlight the importance of developing regulatory frameworks that encourage strategic approaches to cybersecurity rather than prescribing specific technical controls. The strong relationship between strategy and investment suggests that regulations promoting comprehensive security planning may be more effective than narrowly defined compliance requirements. Additionally, the varying patterns observed across industry sectors suggest that regulatory approaches should be tailored to sector-specific dynamics, with particular attention to critical infrastructure sectors where risk management and regulatory factors have stronger direct influences on investment decisions.

The ASEAN Cybersecurity Cooperation Strategy 2021–2025 aims to strengthen and harmonize regional cyber policies while enhancing capacity building (ASEAN, 2023). Our findings suggest that these efforts should focus on promoting strategic planning capabilities within organizations while accommodating sector-specific needs. The multi-group analysis revealing stronger compliance effects in critical infrastructure sectors indicates that targeted regulatory approaches for these sectors may be particularly effective, while broader frameworks supporting strategic development may be more appropriate for other industries.

5.3 Contextual implications for ASEAN organizations

The ASEAN region's diverse economic, technological, and regulatory landscape creates unique challenges for cybersecurity management. Figure 4 presents findings reveal several important implications specific to this regional context.

First, the strong influence of financial considerations on strategy development ($\beta = 0.57$) reflects the resource constraints faced by many ASEAN organizations, particularly in emerging economies. As digital transformation accelerates across the region, organizations must carefully balance security investments against other priorities, making strategic alignment essential for effective resource allocation. This dynamic is particularly evident in countries like Indonesia, Vietnam, and the Philippines, where digital adoption is growing rapidly but resources for cybersecurity remain limited compared to more developed economies like Singapore.

Regional initiatives to enhance cybersecurity capacity should address these financial constraints, potentially through subsidies, tax incentives, or public-private partnerships that reduce financial barriers to essential security measures. The ASEAN Digital Masterplan, developed to suggest actions governments and regulators can take to achieve the vision of ASEAN as a leading digital community (ASEAN, 2023), should incorporate specific measures to support security investments through financial incentives and resource pooling, particularly for smaller organizations and emerging markets within the region.

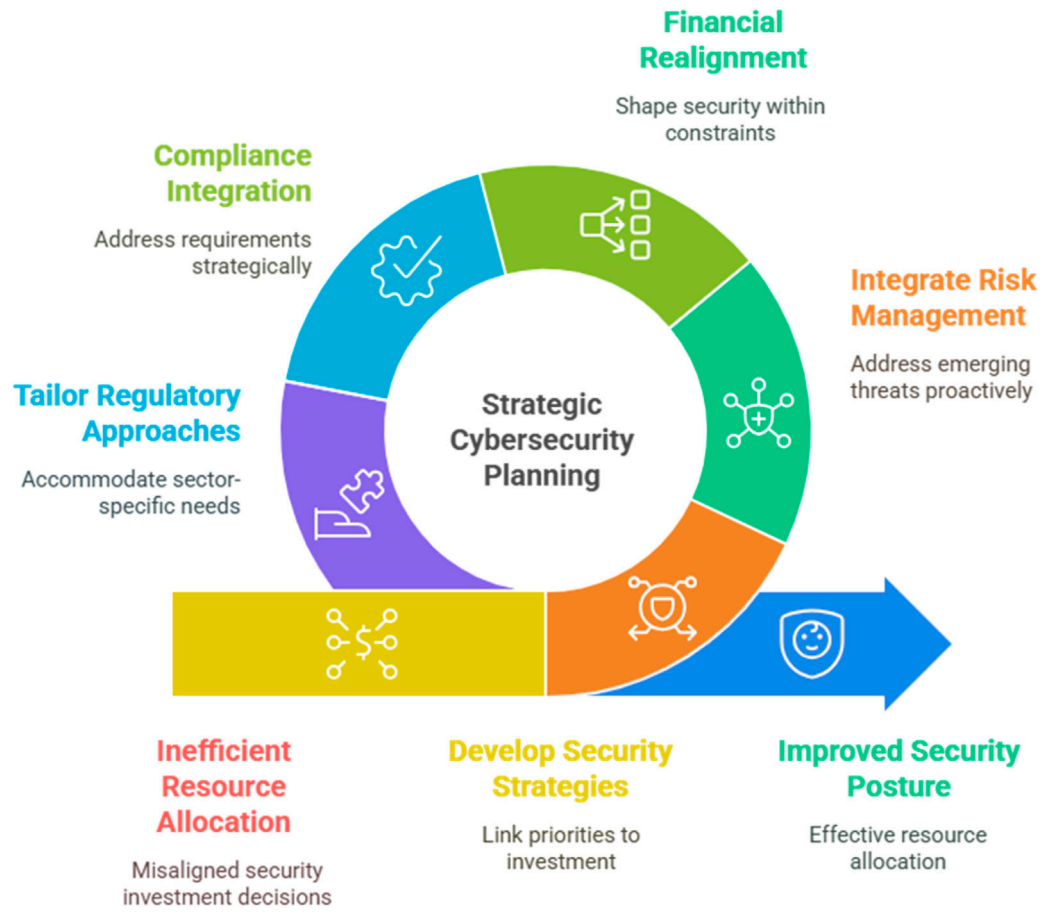

FIGURE 3
Enhancing cybersecurity through strategic planning in ASEAN.

Second, the significant influence of regulatory factors on both strategy ($\beta = 0.42$) and investment ($\beta = 0.19$) highlights the importance of developing regionally appropriate regulatory frameworks that account for varying levels of digital maturity. The ASEAN Cybersecurity Cooperation Strategy provides a foundation for such frameworks, but our findings suggest that implementation should be tailored to specific national and sectoral contexts rather than applying uniform approaches across the region.

Countries like Singapore have developed sophisticated regulatory frameworks through agencies like the Cybersecurity Agency of Singapore, while others are still establishing basic cybersecurity regulations. Our finding that regulatory factors influence investment both directly and through strategy development suggests that regulators across ASEAN should focus not only on compliance requirements but also on promoting strategic planning capabilities within organizations. This dual approach would address both immediate compliance needs and longer-term security development objectives, accommodating the varying regulatory maturity levels across the region.

Third, the multi-group differences observed between critical infrastructure and other sectors underscore the need for sector-specific security approaches within ASEAN. Critical infrastructure protection requires particular attention, with our findings suggesting that organizations in these sectors respond more strongly to risk management considerations and regulatory guidance. Regional coordination mechanisms should prioritize critical infrastructure protection while developing supportive frameworks for other sectors that address their unique decision-making patterns.

The ASEAN Defense Ministers' Meeting Cybersecurity and Information Centre of Excellence (ACICE), established in 2021, and the ASEAN Cyber Defense Network (ACDN) represent important regional initiatives for sharing cybersecurity information and enhancing collective capabilities (CSIS, 2023). Our findings suggest that these initiatives should incorporate sector-specific working groups, particularly for critical infrastructure, to address the different investment determinants and decision patterns observed across sectors.

Fourth, the consistent relationship between strategy and investment across organizational contexts suggests that initiatives to enhance strategic security planning capabilities could significantly improve cybersecurity postures throughout the region. Capacity-building programs focused on strategic planning methodologies, risk assessment frameworks, and investment prioritization techniques could help organizations across the ASEAN region develop more effective approaches to security resource allocation. This recommendation aligns with the capacity-building dimension of the ASEAN Cybersecurity Cooperation Strategy, which

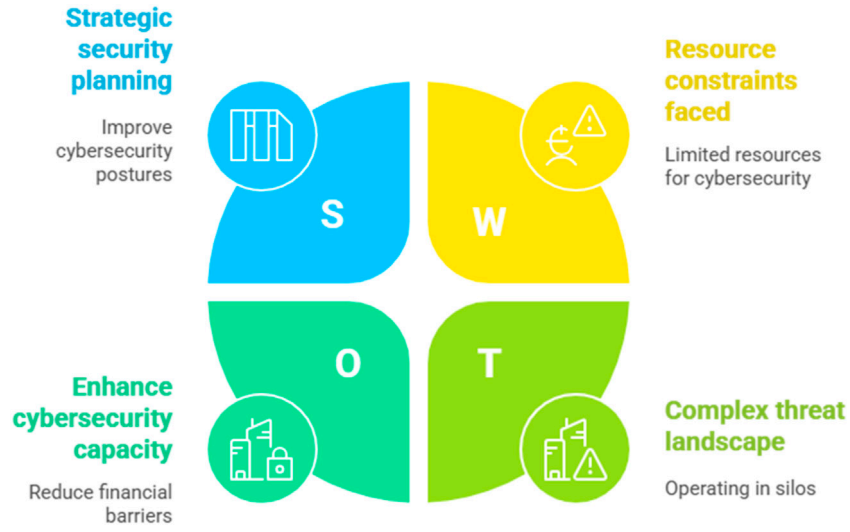

FIGURE 4
ASEAN cybersecurity management.

emphasizes the need for "continued training not only on technical and operational matters, but also on cybersecurity policy, legislation, and strategy" (ASEAN, 2023).

Fifth, our country-specific analyses, though not reaching statistical significance in multi-group comparisons, revealed interesting patterns that reflect ASEAN's diversity. Singapore-based organizations showed slightly stronger relationships between governance factors and investment decisions, consistent with the country's more mature regulatory environment and leadership role in regional cybersecurity initiatives. Organizations from emerging digital economies like Indonesia and Vietnam demonstrated stronger relationships between financial considerations and strategy, potentially reflecting greater resource constraints in these markets. These patterns highlight the importance of considering national contexts when implementing regional cybersecurity frameworks, even as ASEAN pursues greater integration and harmonization.

Finally, the mediation patterns observed across different factors highlight the importance of developing integrated approaches to cybersecurity that connect risk management, financial planning, and regulatory compliance through coherent strategic frameworks. Organizations across ASEAN should ensure that these different functional areas collaborate effectively in developing cybersecurity strategies, rather than operating in silos. This integrated approach is particularly important given the resource constraints and complex threat landscape facing many ASEAN organizations, requiring efficient coordination to maximize security outcomes within available resources.

5.4 Limitations and future research

While our study provides valuable insights into cybersecurity investment determinants in ASEAN organizations, several limitations should be acknowledged. First, our cross-sectional design captures relationships at a specific point in time, limiting our ability to observe how investment patterns evolve in response to changing threats and regulatory environments. Future research could adopt longitudinal approaches to examine the dynamic nature of security investment decisions over time, particularly as ASEAN countries continue to develop their digital economies and regulatory frameworks.

Second, our reliance on self-reported measures may introduce common method bias, although our validation procedures and strong psychometric properties mitigate this concern. Future studies could incorporate objective investment data and organizational security outcomes to strengthen causal inferences and examine the effectiveness of investment decisions in improving security postures. This could include analysis of actual security spending figures, incident metrics, and performance outcomes to assess the relationship between investment patterns and security effectiveness.

Third, while our sample provides broad representation across the ASEAN region, more granular country-level analysis was not feasible due to uneven distribution of respondents across member states. Future research could explore how national contexts within ASEAN influence cybersecurity investment patterns, particularly considering the varying regulatory maturity and digital development stages across the region. Comparative studies focusing specifically on differences between advanced digital economies like Singapore and emerging markets like Vietnam or Cambodia could provide valuable insights into how national contexts shape security investment decisions.

Fourth, our study focused primarily on medium and large organizations with established cybersecurity functions. Future research could extend this investigation to smaller enterprises, which comprise a significant portion of ASEAN's business landscape but often face distinct challenges in cybersecurity resource allocation. The dynamics of investment decision-making likely differ in these smaller organizations, which typically have more limited resources and less formalized security functions.

Fifth, while our model demonstrated strong explanatory power (R^2 = 0.68 for investment), additional factors not included in our framework may also influence investment decisions. Future research could explore additional determinants such as organizational culture, leadership characteristics, competitive pressures, and industry-specific threat profiles. Integrating these factors into more comprehensive models could further enhance understanding of cybersecurity investment dynamics in the ASEAN context.

Finally, our study focused primarily on the determinants of investment decisions rather than their outcomes. Future research could examine the relationship between different investment patterns and cybersecurity performance, including both technical security metrics and broader business outcomes. This could help organizations optimize their investment approaches by identifying which patterns yield the most effective security improvements and business benefits, particularly in ASEAN's diverse operational contexts.

6 Conclusion

This study investigated the factors influencing cybersecurity investment decisions in organizations across the ASEAN region through structural equation modeling of data collected from 317 cybersecurity and IT executives. Our research examined how risk management practices, financial considerations, and regulatory compliance influence investment patterns, both directly and through the mediating role of cybersecurity strategy. The results provide several important insights that advance both theoretical understanding and practical approaches to cybersecurity resource allocation in this diverse regional context.

The findings confirm that cybersecurity strategy serves as the primary determinant of investment decisions ($\beta = 0.63$, $p < 0.001$), acting as a critical mediating variable that translates organizational priorities into resource allocation patterns. This strategic orientation is significantly influenced by financial considerations ($\beta = 0.57$, $p < 0.001$), risk management practices ($\beta = 0.54$, $p < 0.001$), and regulatory frameworks ($\beta = 0.42$, $p < 0.001$), highlighting the multidimensional nature of strategic security planning in ASEAN organizations. The integration of these diverse influences into coherent strategic frameworks appears essential for effective security resource allocation in the region's complex and rapidly evolving digital landscape.

Our analysis revealed distinct mediation patterns that clarify how different factors shape investment decisions. Financial considerations influence cybersecurity investment exclusively through strategy development (full mediation), suggesting that economic factors primarily shape how organizations conceptualize and prioritize their security approaches rather than directly constraining investment decisions. In contrast, both risk management and governance/compliance factors affect investment through dual pathways: directly influencing resource allocation ($\beta = 0.29$ and $\beta = 0.19$, respectively) while also shaping strategic planning processes that subsequently guide investment decisions.

The multi-group analysis demonstrated significant contextual variations in how these relationships manifest across different industry sectors. Organizations in critical infrastructure sectors showed stronger direct relationships between risk management and investment as well as between governance/compliance and both strategy and investment compared to organizations in other sectors. These differences highlight the importance of developing sector-specific approaches to cybersecurity governance and investment that account for varying risk profiles, regulatory requirements, and operational contexts.

The model demonstrated robust explanatory power, accounting for 68% of the variance in cybersecurity investment decisions and 57% of the variance in cybersecurity strategy. This strong explanatory capability validates our integrated theoretical framework and confirms its relevance for understanding security resource allocation in ASEAN's diverse organizational landscape. The consistency of core relationships across organization size categories, coupled with significant variations across industry sectors, suggests that sector-specific dynamics may be more influential than organizational scale in determining investment patterns within the region.

These findings contribute to both academic knowledge and practical application by providing a comprehensive framework that explains how different organizational factors interact to shape cybersecurity investment decisions in a regional context characterized by varying levels of digital maturity and regulatory environments. For researchers, the study advances theoretical integration by demonstrating how distinct perspective risk management, financial decision theory, regulatory compliance, and strategic management—collectively explain investment patterns with substantial explanatory power. For practitioners, the findings offer evidence-based guidance for developing more effective approaches to security resource allocation that balance risk management imperatives, financial constraints, and compliance requirements within coherent strategic frameworks.

For policymakers across the ASEAN region, our results highlight the importance of developing regulatory approaches that encourage strategic security planning while accounting for sector-specific dynamics. The stronger influence of regulatory factors in critical infrastructure sectors suggests that targeted regulatory frameworks for these essential services may be particularly effective, while broader approaches may be appropriate for other sectors where financial considerations play a more dominant role in shaping security strategies.

As the ASEAN region continues its digital transformation journey, organizations face increasing challenges in allocating limited resources to address evolving cybersecurity threats amid diverse regulatory requirements and varying levels of digital maturity. The ASEAN Cybersecurity Cooperation Strategy 2021–2025, which focuses on "advancing cyber readiness, strengthening and harmonizing regional cyber policies, enhancing trust in cyberspace, and regional capacity building" (CSIS, 2023), provides an important framework for addressing these challenges. Our research complements this strategy by providing empirically validated insights into how organizations navigate investment decisions within this complex regional landscape.

This research provides a foundation for understanding how organizations navigate these complex decisions, offering insights that can help enhance cybersecurity resilience across the region. By developing more nuanced approaches to security investment that integrate risk management, financial considerations, and regulatory

compliance within comprehensive strategic frameworks, ASEAN organizations can better protect their digital assets while supporting sustainable economic development throughout the region.

Future research should build on these findings by examining how cybersecurity investment patterns evolve over time, exploring country-specific variations within the ASEAN region, incorporating objective measures of investment effectiveness, and investigating how emerging technologies influence security resource allocation. These extensions would further enhance understanding of cybersecurity investment dynamics in this critical and rapidly developing regional context, contributing to stronger digital resilience across Southeast Asia's diverse economies.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

PR: Writing – original draft, Writing – review and editing, Conceptualization, Methodology. NS: Writing – review and editing, Visualization, Validation. SD: Conceptualization, Supervision, Writing – review and editing, Validation.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

AlDaajeh, S., and Alrabaee, S. (2024). Strategic cybersecurity. *Comput. Secur.* 141, 103845. doi:10.1016/j.cose.2023.103845

Aldasoro, I., Gambacorta, L., Giudici, P., and Leach, T. (2022). The drivers of cyber risk. *J. Financial Stab.* 60, 100989. doi:10.1016/j.jfs.2021.100989

Ali, N., and Lwanga, J. (2023). Cybersecurity strategy implementation in healthcare organizations: a framework for protecting patient data. *J. Healthc. Inf. Manag.* 37 (2), 85–97. doi:10.1142/S0219622023500336

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., and Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: the mediating and moderating role of cybersecurity resilience and organizational culture. *Sustainability* 16 (5), 1880. doi:10.3390/su16051880

ASEAN. (2023). *SEAN Cybersecurity Cooperation Strategy 2021-2025*. Jakarta, Indonesia: ASEAN Secretariat. Available online at: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Bagozzi, R. P., and Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74–94. doi:10.1007/BF02723327

Bharat, P., and Banerjee, J. (2023). Strengthening the legal frameworks of data piracy and cybersecurity in digital era. *Int. J. Law Manag.* 65 (4), 187–199. doi:10.1108/IJLMA-08-2022-0167

Bujang, M. A., Omar, E. D., and Baharum, N. A. (2018). A review on sample size determination for Cronbach's alpha test: a simple guide for researchers. *Malays. J. Med. Sci.* 25 (6), 85–99. doi:10.21315/mjms2018.25.6.9

Caballero-Anthony, M., and Gong, L. (2021). ASEAN-China cybersecurity cooperation: challenges and opportunities. *RSIS Monogr. NTU*. doi:10.26199/20z5-8t15

Celeny, D., Maréchal, L., Rousselot, E., Mermoud, A., and Humbert, M. (2023). Prioritizing investments in cybersecurity: empirical evidence from an event study on the determinants of cyberattack costs. *Inf. Secur.* 54 (1), 94–112. doi:10.11610/isij.5409

Center for Strategic and International Studies (CSIS) (2023). ASEAN's cyber initiatives: a select list. Available online at: https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list.

CompTIA (2022). 2022 state of cybersecurity - ASEAN. Available online at: https://connect.comptia.org/content/research/2022-state-of-cybersecurity—asean.

Faul, F., Erdfelder, E., Buchner, A., and Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: tests for correlation and regression analyses. *Behav. Res. Methods* 41 (4), 1149–1160. doi:10.3758/BRM.41.4.1149

Folorunso, A., Wada, I., Samuel, B., and Mohammed, V. (2022). Security compliance and its implication for cybersecurity. *J. Cybersecurity Priv.* 2 (4), 766–784. doi:10.3390/jcp2040039

Fornell, C., and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* 18 (1), 39–50. doi:10.2307/3151312

Hasani, T., Bojnec, Š., and Ruiz-Alba, J. L. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Bus. & Econ.* 3 (5), 1–29. doi:10.1007/s43546-023-00477-6

Henseler, J., Ringle, C. M., and Sarstedt, M. (2023). The heterotrait-monotrait ratio of correlations: a new criterion for assessing discriminant validity in structural equation modeling. *J. Acad. Mark. Sci.* 51 (2), 443–458. doi:10.1007/s11747-022-00894-3

Héroux, S., and Fortin, A. (2022). The influence of corporate governance mechanisms and contextual factors on cybersecurity disclosure. *J. Inf. Syst.* 36 (1), 195–219. doi:10.2308/ISYS-19-054

Hossain, S. T., Yigitcanlar, T., Nguyen, K., and Xu, Y. (2023). Local government cybersecurity landscape: a systematic review and conceptual framework. *Appl. Sci.* 14 (1), 5501. doi:10.3390/app14135501

Kartal, M. T., Pata, U. K., and Alola, A. A. (2022). Energy security risk and financial development nexus: disaggregated level evidence from South Korea by cross-quantilogram approach. *Appl. Energy* 321, 119322. doi:10.1016/j.apenergy.2022.119322

Kostelić, K. (2024). Dynamic awareness and strategic adaptation in cybersecurity: a game-theory approach. *Games* 15 (2), 13. doi:10.3390/g15020013

Li, Y., Shi, D., and Cai, Z. (2021). The impact of cybersecurity investment on firm value: evidence from a quasi-natural experiment in China. *Asia-Pacific J. Account. Econ.* 30 (1), 1–29. doi:10.1080/16081625.2021.1922753

Liu, C., and Babar, M. A. (2024). Corporate cybersecurity risk and data breaches: a systematic review of empirical research. *Aust. J. Manag.* 49 (2), 1293658. doi:10.1177/03128962241293658

Market Report Analytics (2024). ASEAN cybersecurity industry unlocking growth opportunities: analysis and forecast 2025-2033. Available online at: https://www.marketreportanalytics.com/reports/asean-cybersecurity-industry-89578.

Mazumder, S., and Hossain, M. M. (2023). Board gender diversity and cybersecurity risk disclosure in corporate governance statements. *Account. Finance* 63 (3), 893–922. doi:10.1111/acfi.12956

Mazzoccoli, A. (2023). Optimal cyber security investment in a mixed risk management framework: examining the role of cyber insurance and expenditure analysis. *Risks* 11 (9), 154. doi:10.3390/risks11090154

Melaku, H. M., Ahmed, Z., Qiu, H., and Zhao, Y. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks* 11 (6), 109. doi:10.3390/risks11060109

Pattnaik, N., Tonge, A. M., and Cordeiro, J. (2023). Cybersecurity risks for critical national infrastructure: a systematic literature review. *Comput. Secur.* 127, 103082. doi:10.1016/j.cose.2023.103082

Positive Technologies (2023). Cybersecurity threatscape of Asia: 2022–2023. Available online at: https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/.

Ramadhan, I. (2022). ASEAN consensus and forming cybersecurity regulation in Southeast Asia. *Proceedings of the 1st International Conference on Contemporary Risk Studies*, Bandung, Indonesia: ICONIC-RS 2022, 31 March-1 April 2022. doi:10.4108/eai.31-3-2022.2320684

Ramazonov, I. (2022). Financial institutions cybersecurity standards: legal implications of evolving judicial interpretation of reasonable security measures. *Bank. Law J.* 139 (7), 376–392. doi:10.2139/ssrn.4044868

Rios Insua, D., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., and Rasines, D. G. (2021). An adversarial risk analysis framework for cybersecurity. *Risk Anal.* 41 (1), 16–36. doi:10.1111/risa.13331

Rupra, S. S. (2023). A holistic approach for cybersecurity in organizations. *Sci. Pract. Cyber Secur. J.* 7 (4), 32–39. doi:10.51233/SPCSI.2023.7.4-32

Savaş, S., and Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *Int. Cybersecurity Law Rev.* 3 (1), 7–34. doi:10.1365/s43439-021-00045-4

Smaili, N., Arroyo, P., and Héroux, S. (2023). Board attributes, shareholder confidence, and cyber-security disclosure. *Int. J. Account. Inf. Manag.* 31 (1), 116–138. doi:10.1108/IJAIM-05-2022-0093

Springermann, K., Ramazonov, I., and Porrini, D. (2024). More than malware: unmasking the hidden risk of cybersecurity regulations. *Int. Cybersecurity Law Rev.* 2024, 1–19. doi:10.1365/s43439-024-00111-7

Sukma, N., and Leelasantitham, A. (2022). Understanding online behavior towards community water user participation: a perspective of a developing country. *PloS one* 17 (7), e0270137. doi:10.1371/journal.pone.0270137

Sukma, N., and Leelasantitham, A. (2022a). A community sustainability ecosystem modeling for water supply business in Thailand. *Front. Environ. Sci.* 10, 940955. doi:10.3389/fenvs.2022.940955

Sukma, N., and Leelasantitham, A. (2022b). From conceptual model to conceptual framework: a sustainable business framework for community water supply businesses. *Front. Environ. Sci.* 10, 1013153. doi:10.3389/fenvs.2022.1013153

Sukma, N., and Leelasantitham, A. (2022c). The influence and continuance intention of the E-government system: a case study of community water supply business. *Front. Environ. Sci.* 10, 918981. doi:10.3389/fenvs.2022.918981

Sukma, N., Leelasantitham, A., and Yan, Z. (2022). Factors affecting adoption of online community water user participation. *Hum. Behav. Emerg. Technol.* 2022 (1), 1–13. doi:10.1155/2022/1732944

Sukma, N., and Namahoot, C. S. (2024a). An algorithmic trading approach merging machine learning with multi-indicator strategies for optimal performance. *IEEE Access* 12, 188154–188173. doi:10.1109/access.2024.3516053

Sukma, N., and Namahoot, C. S. (2024b). Enhancing trading strategies: a multi-indicator analysis for profitable algorithmic trading. *Comput. Econ.* 48. doi:10.1007/s10614-024-10669-3

Sukma, N., and Namahoot, C. S. (2025). Predictive modeling for identifying undervalued stocks using machine learning. *Int. J. Inf. Technol. Decis. Mak.* 1–26. doi:10.1142/s0219622025500336

Sukma, N., and Namahoot Chakkrit, S. (2024). Trading strategies development using combined enhanced voter-method with technical indicators and machine learning. *ICIC Express Lett. Part B Appl.* 15 (05), 427. doi:10.24507/icicelb.15.05.427

Sukma, N., and Pum, W. (2025). BEST: an instructional design model to empower graduate student self-efficacy in research. *Interdiscip. J. Inf. Knowl. Manag.*, 20, 010. doi:10.28945/5476

Sukma, N., and Yamnill, S. (2025). Future economic and sustainability impacts of open data in insurance. *Public Adm. Issues* 0 (5), 131–158. doi:10.17323/1999-5431-2025-0-5-131-158

Tetteh, G. K., and Otioma, C. (2022). Cyberattack, cyber risk mitigation capabilities, and firm productivity in emerging economies. *Small Bus. Econ.* 59 (3), 1045–1067. doi:10.1007/s11187-021-00572-8

Zhang, H., Li, Y., Wang, H., and Yin, L. (2023). Corporate investment reactions to external security risks: evidence from cyber threats. *Res. Int. Bus. Finance* 66, 101974. doi:10.1016/j.ribaf.2023.101974

Zuhroh, N. F., and Baihaqy, A. (2023). Examining the readiness of the organization's security success in improving security performance. *J. Comput. Secur.* 11 (3), 545–560. doi:10.15408/jcs.v11i3.28574