Contents lists available at GrowingScience

Management Science Letters

homepage: www.GrowingScience.com/msl

Influential factors of cybersecurity investment: A quantitative SEM analysis

Phasikha Rattanapong[a*] **and Smitti Darakorn Na Ayuthaya**[a]

[a] *Technology of Information System Management Division, Faculty of Engineering, Mahidol University, Nakhonpathom, Thailand*

CHRONICLE

Article history:
Received: December 20, 2023
Received in revised format:
January 26 2024
Accepted: March 17, 2024
Available online:
March 17 2024

Keywords:
Cybersecurity Investment
Resilience
Structural Equation Modeling (SEM)
Risk Assessment
Organizational Resilience

ABSTRACT

In the dynamic landscape of digital enterprises, cybersecurity has emerged as a critical determinant of organizational effectiveness. This study delves into the intricate realm of cybersecurity investment within ASEAN organizations, exploring the key facets that drive decision-making in this domain. Using a quantitative approach through structural equation modeling (SEM), we conducted an in-depth analysis based on a sample of 419 enterprises meeting cybersecurity criteria. Our findings reveal that cybersecurity strategy, financial considerations, and institutional and regulatory conditions are the primary factors influencing cybersecurity investments in the ASEAN region. In particular, financial resources emerged as the most critical determinant, underscoring the importance of adequate funding to address evolving cyber threats. Furthermore, our study highlights the crucial role of institutional and regulatory frameworks in shaping investment behavior, indicating a heightened awareness among firms regarding compliance with legal requirements. By unpacking these dynamics, our research provides deep insights into the intricate interplay of factors shaping cybersecurity investments in ASEAN organizations. This study contributes to the discourse by emphasizing the imperative nature of understanding the impact of risk aversion, organizational structures, and long-term practices on cybersecurity resilience. The implications of our findings extend to policy making, innovation, and future research directions in the cybersecurity domain, offering valuable insights to improve cybersecurity preparedness and resilience against evolving cyber threats.

© 2025 by the authors; licensee Growing Science, Canada

1. Introduction

In the rapidly evolving digital landscape, cybersecurity has become a cornerstone of organizational resilience, particularly in the context of the Association of Southeast Asian Nations (ASEAN) region. With the increasing frequency and sophistication of cyber threats, ASEAN organizations are faced with unique challenges that require a strategic approach to cybersecurity investment. Understanding the specific cybersecurity challenges faced by organizations in ASEAN is crucial to developing effective risk mitigation strategies and improving overall cybersecurity resilience. The ASEAN region, which comprises ten different member states, is a vibrant economic hub characterized by rapid technological advances and digital transformation. As organizations in ASEAN embrace digital technologies to drive innovation and growth, they are also exposed to a myriad of cybersecurity risks that threaten the integrity of their operations, data, and reputation(Gordon et al., 2003) From sophisticated cyberattacks targeting critical infrastructure to data breaches that compromise sensitive information, the cybersecurity landscape in ASEAN is dynamic and complex (Tran Dai & Gomez, 2018). One of the key cybersecurity challenges facing organizations in the ASEAN region is the evolving nature of cyber threats. Cyber adversaries are constantly adapting their tactics to exploit vulnerabilities in organizational systems and networks, posing a significant risk to data security and business continuity (Mohamed Mizan et al., 2019). Furthermore, the interconnected nature of digital ecosystems in ASEAN amplifies

* Corresponding author.

E-mail address: phasikha.rat@student.mahidol.ac.th (P. Rattanapong)

© 2025 by the authors; licensee Growing Science, Canada
doi: 10.5267/j.msl.2024.3.005

the impact of cyber incidents, underscoring the need for robust cybersecurity measures to protect against potential disruptions (Corallo et al., 2020a). Another critical cybersecurity challenge in the ASEAN region is the shortage of skilled cybersecurity professionals. As organizations strive to enhance their cybersecurity capabilities, the demand for qualified cybersecurity experts far exceeds the available talent pool (Aksoy, 2024; Cao, 2023). These skills gaps not only hinder the effective implementation of cybersecurity strategies, but also leave organizations vulnerable to cyber threats due to a lack of specialized expertise in detecting and mitigating security incidents.

In response to these challenges, ASEAN organizations are increasingly recognizing the importance of investing in cybersecurity to protect their digital assets and maintain operational resilience. Cybersecurity investment encompasses a wide range of activities, including the deployment of security technologies, the implementation of security policies and procedures, and the training of employees to improve cybersecurity awareness and best practices (Aksoy, 2024; AlDaajeh et al., 2022). By allocating resources to cybersecurity initiatives, organizations can strengthen their defenses against cyber threats and mitigate the potential impact of security breaches.

Then we lead to the Research Question:

- What factors drive cybersecurity investment decisions in ASEAN organizations and how do they impact cybersecurity resilience?

To address the complex interplay of factors influencing cybersecurity investment decisions in the ASEAN region, this study adopts a quantitative approach through structural equation modeling (SEM). SEM is a powerful statistical technique that allows researchers to analyze complex relationships between multiple variables and test theoretical models of causality (Kline, 2023). By applying SEM to the study of cybersecurity investment in ASEAN organizations, our goal is to uncover the underlying factors that drive investment decisions and shape cybersecurity strategies in this diverse and dynamic region. The importance of conducting a quantitative analysis through SEM lies in its ability to provide a rigorous and systematic examination of the factors that influence cybersecurity investment in ASEAN. By quantifying the relationships between cybersecurity strategy, financial considerations, institutional and regulatory conditions, risk assessment, and organizational elements, we can gain valuable insights into the determinants of cybersecurity investment decisions and their implications for organizational resilience (Cao, 2023; Tran Dai & Gomez, 2018).

2. Theoretical background

Cybersecurity investment has become a critical priority for organizations around the world, particularly in the region of the dynamic landscape of the Association of Southeast Asian Nations (ASEAN). As digital transformation accelerates and cyber threats evolve in complexity and frequency, understanding the factors driving cybersecurity investment decisions in ASEAN organizations is paramount to improve resilience and safeguarding critical assets. This review of the literature provides a comprehensive analysis of key themes and empirical evidence related to cybersecurity investment in the ASEAN context, drawing on theoretical frameworks and practical insights to guide the research study (Gordon et al., 2003; Gordon et al., 2020; Tsohou et al., 2008).

2.1 Cybersecurity Investment Landscape in ASEAN

The ASEAN region, which comprises ten different member states, is a burgeoning economic hub characterized by rapid technological advancements and digital innovation. With the increasing adoption of digital technologies across industries, organizations in ASEAN face a myriad of cybersecurity challenges that require strategic investments in cybersecurity measures. From data breaches and ransomware attacks to supply chain vulnerabilities and regulatory compliance issues, the cybersecurity landscape in ASEAN is multifaceted and requires a proactive approach to risk mitigation. (Tran Dai & Gomez, 2018)

2.2 Factors Influencing Cybersecurity Investment Decisions

Several key factors drive cybersecurity investment decisions in ASEAN organizations, shaping their approach to cybersecurity strategy and resource allocation. Risk assessment, financial considerations, legal frameworks, business models, and organizational structures play a crucial role in determining the extent and effectiveness of cybersecurity investments. Understanding the interaction between these factors is essential to develop robust cybersecurity strategies that align with organizational objectives and improve resilience against evolving (Barney, 2016) cyber threats. (Gordon & Loeb, 2002; Sonnenreich et al., 2006)

2.3 Theoretical Perspectives on Cybersecurity Investment

The resource-based view (RBV) theory offers valuable insight into how organizations in the ASEAN region can leverage their internal resources and capabilities to make strategic cybersecurity investments. By identifying and mobilizing valuable assets such as a skilled workforce, technological infrastructure, and regulatory compliance frameworks, organizations can improve their cybersecurity posture and competitive advantage in the digital marketplace. The RBV theory underscores the importance of aligning cybersecurity investments with organizational strengths and strategic priorities to achieve sustainable cybersecurity resilience. (Barney, 2016; Barney, 1986; Bharadwaj, 2000)

2.4 Implications for Cybersecurity Investment

Policymaking in ASEAN organizations and governments plays a crucial role in shaping cybersecurity investment decisions and fostering a culture of cyber resilience. By aligning corporate policies with the variables that influence cybersecurity investments, policymakers can promote the adoption of rigorous risk assessment frameworks, cybersecurity education initiatives, and privacy regulations that improve data protection and cybersecurity awareness. Encouraging firms to invest in innovative cybersecurity solutions through research and development initiatives can further improve cybersecurity resilience and mitigate cyber risks in the ASEAN region.(Gordon et al., 2020; Lee, 2021; Romanosky et al., 2014; Tran Dai & Gomez, 2018)

2.5 Innovation in Cybersecurity Investment

Organizations in ASEAN exhibit a distinctive approach to cybersecurity investment compared to counterparts in other regions, emphasizing the importance of customer trust, risk awareness, and robust cybersecurity measures. Although ASEAN entities maintain a certain level of security, it is a need to adapt to the rapidly evolving technological landscape and embrace cybersecurity innovations to improve resilience and digital capabilities. By fostering a culture of innovation and embracing emerging technologies, ASEAN organizations can position themselves for global competitiveness and sustainable growth in the digital age. (Abrahams et al., 2024; Aksoy, 2024; Luiijf et al., 2013).

2.6 Legal Factors

Legal and regulatory constraints profoundly shape cybersecurity investment decisions, as noted by Becker (1968) and Fleury (2017)(Fleury, 2017). Compliance with legal obligations not only mitigates risks, but also avoids potential fines (Shavell, 1984). The legal and regulatory environment hypothesis posits that these legal mandates influence firms' investment behaviors, offering both responsibilities and incentives (Galbiati & Vertova, 2014). For example, privacy regulations necessitate specific security measures to protect client data. Additionally, regulatory requirements, such as public disclosures, impact organizational performance after cyber incidents (Corallo et al., 2020b; Fleury, 2017).

This study explores the risk, organizational dynamics, cybersecurity strategy, financial aspects, and legal factors that influence cybersecurity investments, using the Resource-Based View (RBV) framework (Barney, 2016; Barney, 1986). By prioritizing cybersecurity, ASEAN organizations can efficiently allocate resources and strengthen defenses against cyber threats, contributing to the region's cybersecurity discourse.

Table 3
Summarized factors from the related study.

Variables	Description	Factors	References
Risk	Cyber threats can harm organizations' data, systems, and assets. Identifying, assessing, and mitigating risks is necessary to prevent or minimizing cyberattacks.	Competitive advantage Insurance Loss Risk management Vulnerabilities	(Bodin et al., 2018; Kamiya et al., 2021; Slovic, 1987; Thekdi & Aven, 2019)
Business / Organization	Cybersecurity is an important concern because companies and organizations use digital technology. technologies to store and process sensitive data. Cyberattacks can be costly in terms of money, reputation, and legal trouble.	Customer requirement Decision-making process Entrepreneur's Characteristics Management skills Market characteristics Trust - CRM	(Dewett & Jones, 2001; Pfeffer & Salancik, 1978; Sukma & Leelasantitham, 2022)
Cybersecurity Strategy	A cybersecurity strategy describes how an organization protects its data, systems, and assets from cyberattacks. Risk assessment, security controls, and ongoing monitoring and improvement are all part of it.	Cybersecurity strategy Cybersecurity Awareness Investment intentions	(Barney, 1986; Lukavchenko, 2015; Miyamoto et al., 2017)
Financial Consideration	Data breaches lose revenue and reputational damage can be extremely costly for businesses. As a result, organizations must invest in solid cybersecurity to avoid financial losses.	Budget Cost-benefit analysis Economic environment Return on Investment	(Gordon & Loeb, 2002; Gordon et al., 2020; Kissoon, 2020)
Institutional & Regulatory Environment	Organizations must safeguard sensitive data, report breaches, and follow privacy regulations. These rules must be followed to avoid legal and financial implications.	Personal Data Law Impact of Law Fines Regulatory environment	(Abrahams et al., 2024; Fleury, 2017; Galbiati & Vertova, 2014; Shavell, 1984)

3. Research Model and Hypotheses

3.2 Development of hypotheses

We established a conceptual model to examine the various components of cybersecurity investment, as illustrated in Figure 2. This model was developed by synthesizing the literature variables from Table 1 and aligning them with Gordon and Loeb's GL model, which draws upon factors from the Resource-Based View (RBV) theory(Barney, 2016; Erdfelder et al., 1996; Gordon, 2007; Gordon & Loeb, 2002). Subsequently, we introduced additional hypothesis elements to further enrich our analysis. Our research model tested hypotheses regarding the factors influencing cybersecurity investment through H1-H5. By integrating Figure 1 with Table 3, we constructed a comprehensive research model based on our hypotheses, thus creating a robust conceptual framework for our study.

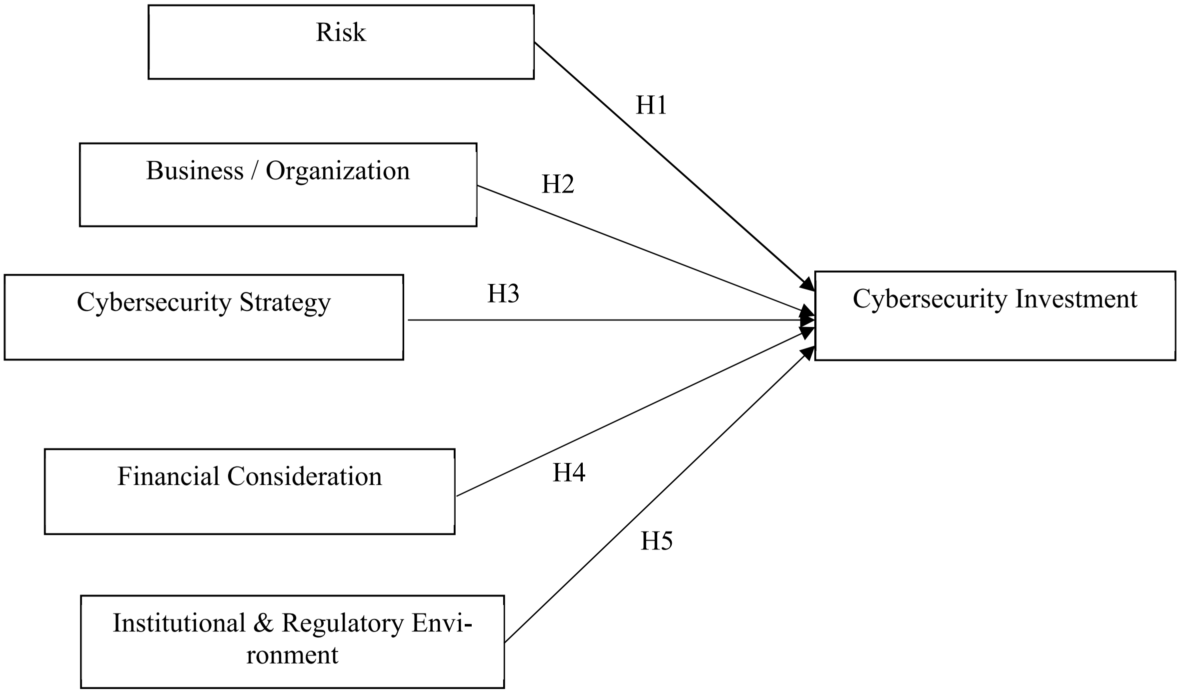


Fig. 1. Research model

Table 1
Hypotheses and Literature Support

Hypothesis	Link	Literature Support
H1:	Risk had influences on cybersecurity investments.	(Bodin et al., 2018; Kamiya et al., 2021; Slovic, 1987)
H2:	Businesses/organizations had influences on cybersecurity investment.	(Hasan et al., 2021; Pfeffer & Salancik, 1978; Sukma & Leelasantitham, 2022)
H3:	The cyber security strategy had influence on Cybersecurity Investment	(Barney, 1986; Miyamoto et al., 2017)
H4:	Financial consideration had influences on Cybersecurity Investment	(Gordon & Loeb, 2002; Gordon et al., 2020; Jensen & Meckling, 1976)
H5:	Institutional & Regulatory Environments had influence on Cybersecurity Investment.	(Abrahams et al., 2024; Fleury, 2017; Shavell, 1984)

To produce questionnaires, we propose factors with details of 15 questions based on the model variables shown in Table 2. These factors included risk, loss, vulnerability, cybersecurity strategy, investment, financial consideration, institutional and regulatory environment, and business or organization.

Table 2
Factors and Variables in the Cybersecurity Investment Research Model

	Factors	1	2	3
RIS	Risk	Risk Assessment	Risk management	Insurance
BUO	Business / Organization	CRM	Management skills	R&D
CYS	Cybersecurity Strategy	Policy	Measurement	Process
FIC	Financial Consideration	Profit	Retention Ratio	ROI
INR	Institutional & Regulatory Environment	State Regulation	Business Regulation	Laws
INVNew	Cybersecurity Investment	The total cost of cybersecurity Investment in 2022		

4. Research Methodology

This study investigated the factors driving the investment of enterprise cybersecurity in the ASEAN area, with a particular emphasis on access. The research question driving this study was: What factors influence enterprises' cybersecurity investment in ASEAN to approve budgets? The research methodology used in this study was a comprehensive approach that encompassed a literature review, the formulation of research questions, the identification of factors, the development and testing of questionnaires, a pilot survey, data collection through an online survey, the exploratory factor analysis (EFA) process, the confirmatory factor analysis (CFA) process, the structural equation modeling (SEM) process, the path analysis and hypothesis testing, interpret the result, discussion and conclusion. This study utilized SPSS and AMOS to analyze the quantitative data: discrete data, count numbers, and continuous data: from Likert's scale: INV, RIS1, RIS2, RIS3, BUO1, BUO2, BUO3 CYS1, CYS2, CYS3, FIC1, FIC2, FIC3, INR1, INR2 and INR3 to investigate the relationship between variables and data in Table 2 to forecast cybersecurity investment.

4.1 Research Design

The research design for this study was based on a quantitative approach using structural equation modeling (SEM). SEM allows for the examination of complex relationships between multiple constructs and latent variables, providing a comprehensive understanding of the factors that affect cybersecurity investment. We proposed 15 items derived from five constructs related to cybersecurity investment.

4.2 Population and sample size

The study population was defined by organizations within the ASEAN region, specifically focusing on enterprises in Thailand and other ASEAN countries.

Population scope: The study targeted individuals at the executive management, cybersecurity, or information technology (IT) management levels, possessing over 10 years of experience in IT, cybersecurity, or Security Operation Center (SOC) roles within their respective organizations. This group included professionals such as chief information officers (CIO), chief technology officers (CTO), IT managers, and regulators. Organizations with more than 50 employees were selected for inclusion in the study due to their potential impact on cybersecurity controls, including factors such as cybersecurity awareness and literacy levels (Dewett & Jones, 2001). Furthermore, the presence of separate IT or cybersecurity departments within these organizations was considered essential for the study focus (Hasan et al., 2021).

4.2.1 Sample size determination

The sample size for this study was determined through a rigorous power analysis process. G*Power version 3.1.9.7 was used to calculate the sample size estimate, considering key parameters such as alpha (α), power (P), degrees of freedom (df) and effect size (Erdfelder et al., 1996; Faul et al., 2007; MacCallum et al., 1996).A total of 317 samples were collected for this investigation, with the Chi-square test utilized based on a significance level of α= 0.05, power of 0.95, df of 16, and effect size of 0.3, as recommended by Cohen (Cohen, 2013). The sample size of 317 observations was deemed necessary for this study, considering the inclusion of 16 variables for factor analysis.

4.2.2 Sampling Strategy

In this study, executives or managers with more than ten years of experience were selected from ASEAN-based firms with IT or cybersecurity divisions and a user base that exceeds 50 individuals. The sampling procedure involved two key steps: Purposive sampling and snowball sampling. Also. The initial stage involved identifying and choosing organizations that met specific inclusion criteria (Etikan et al., 2016). This approach ensured a diverse sample representing various companies in terms of industry, size, and geographical location within the ASEAN region. Selection criteria included the presence of an IT or cybersecurity department and a user base of at least 50 individuals. Although snowball sampling (4.2.2): Following a purposive sampling, referrals from current cybersecurity vendors and partners were leveraged to identify potential respondents from other organizations. This snowball sampling technique expanded the sample size beyond the original firm selection (Biernacki & Waldorf, 1981).

4.3 Data Collection Process

An online survey using Google Forms was used to gather data for the study. Approximately 580 survey links were distributed via email and Messenger to selected organizations. The survey focused on five constructs: risk, organization, financial, legal, and cybersecurity strategy, along with investment in the previous 12 months (fiscal year 2022). Respondents used a Likert scale of 1 to 5 to indicate their agreement or disagreement with the provided statements. Demographic questions were also included to collect relevant information about respondents and their companies.

4.4 Survey Instrument

Data collection was carried out efficiently using a well-designed questionnaire that addressed 15 interconnected ideas considered essential determinants of cybersecurity investment. Likert scale items were incorporated to assess respondents' perspectives on the constructs, along with a question regarding the total cost of cyber security investment in the past 12 months (2022).

4.5 Validity and Reliability

Specialists in cybersecurity and research methods evaluated the validity of the questionnaire's content to ensure clarity and comprehensiveness. The reliability of the questionnaire was assessed using Cronbach's alpha coefficient, with a threshold of 0.6 set for acceptable reliability (Cronbach, 1951; Kline, 2023). The dataset, comprising 16 items, demonstrated strong reliability with a Cronbach's alpha of 0.93, supporting the validity and appropriateness of the research.

5. Results

5.1 Sociodemographic Characteristics of Observations

The online questionnaires were distributed to executives and managers in the information technology (IT) and cybersecurity departments of ASEAN-based firms. The survey link was distributed to around 580 recipients during February and March 2023. A total of 446 responses were received, representing a response rate of 76.9%. After filtering out unauthorized samples, 419 valid responses were retained for data analysis, as detailed in Table 4.

Table 4
Sociodemographic characteristics of observations

		Frequency	**%**
Education Degree	Total	419	100.0%
	Under graduated	15	3.6%
	Graduated	262	62.5%
	Post-Graduated	142	33.9%
Responsibility in Cybersecurity investment	Total	419	100.0%
	Decision- maker	168	40.2%
	Budget creator	161	38.5%
	Requester or User	90	21.3%
Types of organization	Total	419	100.0%
	Government/Government agencies	86	20.6%
	State-owned enterprises	106	25.3%
	Private sector	227	54.1%
Type of your business Industries	Total	419	100.0%
	Policy & Governance	16	3.7%
	Bank/Financial Service/Insurance	55	13.2%
	Telecommunication	55	13.2%
	Education	32	7.7%
	Enterprise/Retails	45	10.7%
	Tourism/Recreation	15	3.5%
	Logistics and Transportation	37	8.8%
	Non-Profit Organization	13	3.2%
	Information Technology	80	19.0%
	Others	71	16.9%
Organization’s location	Total	419	100.0%
	Thailand	287	68.4%
	ASEAN countries	132	31.6%

As shown in Table 4, there were 419 observations in this survey. Sixty-five percent of these organizations have more than 200 users, 54.1% are from the private sector, and the data were divided into 12 categories depending on the types of enterprises that comprise this sector.

5.2. Measurement of Variables and Evaluation of Structural Model

The rotated component matrix revealed varying loads for the five selected components, with significant loadings surpassing 0.5. In particular, INR2, INR3, and INR1 exhibited high loading on component 1, indicating a focus on legal and regulatory aspects. Financial considerations were prominent in FIC3, FIC2, and FIC1, while BUO1, BUO2, and BUO3 demonstrated strong associations with component 3, reflecting organizational structures. Component 4 highlighted the components of the cybersecurity strategy CYS1, CYS3, and CYS2, whereas risk factors RIS3, RIS1, and RIS2 showed a substantial loading on component 5. These results elucidated how the five components contributed to explaining the variance in the data, simplifying the understanding of variable relationships, and confirming the results of the factor analysis.

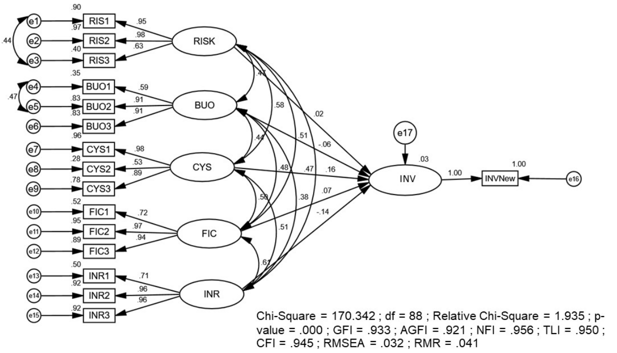
In Table 5, the results of the factor analysis were presented, grouping the elements into constructs based on their correlations. The table displayed the loading of each item onto its corresponding construct, along with metrics such as Cronbach's alpha and CR (critical ratio). High construct reliability indicated internal consistency within the constructs (Bland & Altman, 1997; Henson, 2019; Kline, 2023). A CR value of 0.7 or higher is considered good, although a CR exceeding 0.5 is acceptable, and an AVE (average variance extracted) greater than 0.5 is desirable for each construct. These metrics underscored the robustness and validity of the constructs, supporting the reliability of the factor analysis and confirming the interrelationships among the variables.

Table 5
Model result of loadings, reliability, and validity assessment.

Construct	Item	Loading	Cronbach's alpha	CR.	AVE	Discriminant validity?
Risk			0.900	0.900	0.757	Yes
Risk	RIS1	0.951				
	RIS2	0.982				
	RIS3	0.634				
BUO			0.874	0.855	0.671	Yes
Business and Organization	BUO1	0.594				
	BUO2	0.910				
	BUO2	0.912				
CYS			0.760	0.855	0.676	Yes
Cybersecurity Strategy	CYS1	0.981				
	CYS2	0.530				
	CYS3	0.886				
FIC			0.904	0.915	0.785	Yes
Financial Consideration	FIC1	0.724				
	FIC2	0.972				
	FIC3	0.942				
INR			0.906	0.912	0.780	Yes
Institutional & Regulatory Environment	INR1	0.707				
	INR2	0.957				
	INR3	0.961				

5.3. Structural Equation Modeling Analysis (SEM)

The structural equation modeling (SEM) model depicted in Fig. 2 underwent a comprehensive testing to assess its goodness of fit using a range of fit indices. The Chi-square value of 170.342 highlighted a certain level of discrepancy between the actual data and the model's predictions, with lower values indicating a better fit. It should be noted that the Chi-square test tended to improve with an increase in sample size, enhancing the model's accuracy (Hair et al., 2013). Degrees of freedom (DF) provided information on the calculated model parameters, with a lower CMIN score of 1.930 suggesting an improved alignment between the model and the data among the 88 potential outcomes.



Chi-Square = 170.342 ; df = 88 ; Relative Chi-Square = 1.935 ; p-value = .000 ; GFI = .933 ; AGFI = .921 ; NFI = .956 ; TLI = .950 ; CFI = .945 ; RMSEA = .032 ; RMR = .041

Fig. 2. Results of the SEM Model Analysis

Various goodness-of-fit tests, including GFI, AGFI, NFI, TLI, and CFI, demonstrated strong support for the model, with values ranging from 0.921 to 0.956. Furthermore, the RMSEA value of 0.032 and the RMR value of 0.041 affirmed the model's excellent fit. This alignment with the chi-square test, degrees of freedom, and other goodness-of-fit criteria validates the efficacy of the SEM model, in line with established theoretical hypotheses(Hair et al., 2013; Kline, 2023). These results encourage further exploration of the nuanced implications of the model, shed light on its potential implications and contribute to the advancement of knowledge in the field.

Table 6
SEM statistics indices for measurement model and structural

Statistics	Acceptable fit indices*	Scores	Result
CMIN/DF	< 5.00	0.021	Fit
GFI	≥ 0.90	0.933	Good fit
AGFI	≥ 0.90	0.921	Good fit
NFI	≥ 0.90	0.956	Good fit
TLI	≥ 0.90	0.950	Good fit
CFI	≥ 0.90	0.945	Good fit
RMESEA	< 0.80	0.032	Good fit
RMR	< 0.50	0.041	Good fit

Acceptable fit indices* (Hair et al., 2013; Kline, 2023)

5.4. Hypothesis test of the relationship between two variables (Path analysis)

Table 6 presents the results of a hypothesis test using structural equation modeling (SEM). The test evaluates the relationships between 5 variables, namely Risk, BUO (Business Organization), CYS (Cybersecurity Strategy), FIC (Financial Consideration) and INR (Institutional & Regulatory Environment). The dependent variable in this test was INV (Investment).

Table 7
Results of the hypothesis test of the relationship between two variables.

Hypothesis	*Standardized Beta*	*SE*	*T-value*	*p-values*
Risk → INV	0.025	0.090	0.379	0.705
BUO → INV	-0.059	0.054	-0.963	0.335
CYS→ INV	0.159*	0.067	2.439	0.015*
FIC→ INV	0.246*	0.071	3.694	0.011*
INR → INV	0.135*	0.060	2.053	0.040*

*p<0.05, Risk, BUO (Business Organization), CYS (Cybersecurity Strategy), FIC (Financial Consideration), INR (Institutional & Regulatory Environment), INV (Investment)

Path: A relationship between two variables, one of which was the independent variable and the other was the dependent variable (Fornell & Larcker, 1981; Hancock, 1997; Kline, 2023). B: The estimated coefficient. SE denotes the standard error of the coefficient estimate. The t-value of the coefficient estimate indicated the importance of the path; the p-value of the t-value showed the importance of the path (Hancock, 1997). The significant p-values in this study were those that were less than the standard level of significance, which was 0.05.

Table 8
Summary of Hypothesis Testing on Effects of Factors on Cybersecurity Investment.

Hypothesis		**Result**	**Standardized Beta**
H1	Risk had influences on Cybersecurity Investment	Not supported	0.025
H2	Business/organization had influences on Cybersecurity Investment	Not Supported	-0.059
H3	The Cybersecurity Strategy had influences on the Cybersecurity Investment	Supported	0.159*
H4	Financial Consideration had Influences on Cybersecurity Investment	Supported	0.246*
H5	Institutional and regulatory environment had influences on Cybersecurity Investment	Supported	0.135*

*p<0.05

Tables 7 and 8 reveal significant positive path coefficients ($p < 0.05$) for CYS→INV, FIC→INV, and INR→INV, indicating the impactful influence of cybersecurity strategy, financial considerations, and institutional/regulatory frameworks on investment. On the contrary, the Risk and BUO→INV paths, while positive, lacked statistical significance ($p > 0.05$). Figure 3 underscores CYS, FIC and INR as substantial investment predictors, compared to nonsignificant associations for RISK and BUO. Furthermore, Tables 7 and 8 reaffirm the positive and significant path coefficients ($p < 0.05$) for CYS→INV, FIC→INV, and INR→INV, underscoring the robust influence of cybersecurity strategy, financial considerations, and institutional/regulatory frameworks on investment. Importantly, our findings validate the positive relationship between cybersecurity investment and company value, supporting the significant connection between CYS and Cybersecurity Investment(Anderson & Moore, 2006). Furthermore, the study corroborates the importance of law and Regulation in enhancing cybersecurity investment, aligning with previous research (Romanosky & Acquisti, 2009; Romanosky et al., 2014). These results emphasize the critical role of financial management in shaping investment decisions, contributing to a nuanced understanding of the factors driving organizational performance and value creation.

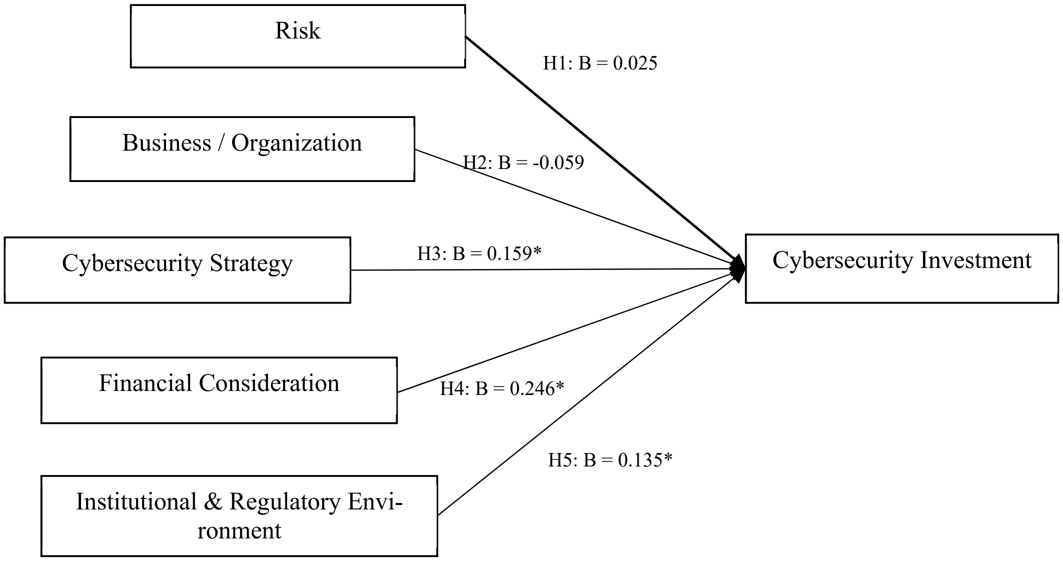


Fig. 3. Results of the research model hypothesis testing.

Based on the results of the hypothesis tests, Fig. 3 revealed that the cybersecurity strategy, financial consideration, and Institutional & Regulatory Environment emerged as significant predictors of investment. At the same time, Risk and Business Organization may have a different significance level.

6. Discussion

The findings of this study shed light on crucial factors influencing companies' decisions regarding cybersecurity investments. Financial considerations emerged as the main driver, with executives prioritizing financial metrics such as ROI, retention ratio, and profit. This aligns with the existing literature that emphasizes the importance of demonstrating the financial benefits of cybersecurity initiatives to stakeholders (Barney, 2016; Barney, 1986). The correlation between financial metrics and budget approval underscores the need for cybersecurity professionals to articulate the economic value and returns associated with their initiatives. Moreover, a notable revelation was the prominence of cybersecurity strategy as a determinant in investment decisions. This includes factors such as awareness, well-defined policies, and prioritization of management. The importance of a proactive approach to cybersecurity is emphasized, aligning with previous research (Barney, 2016; Gordon & Loeb, 2002; Gordon et al., 2020) . Organizations, therefore, must therefore not only invest in technologies but also in developing comprehensive cybersecurity strategies that improve resilience against cyber threats. Furthermore, legal considerations emerged as a significant influence on cybersecurity investments in ASEAN companies, underlining the impact of privacy laws on business performance. This finding emphasizes the need for companies to not only comply with legal requirements, but also manage reputational risks associated with data breaches or cyberattacks (Shavell, 1984). Public scrutiny and legal consequences act as motivating factors for enterprises to allocate resources to cybersecurity initiatives. Furthermore, the study highlighted the importance of comprehensively addressing risk and organizational factors in cybersecurity investment strategies. Practical and effective risk assessment and management practices are essential to identify and mitigate potential cyber threats. Organizational culture, structure, and governance, including board oversight, play a pivotal role in shaping cybersecurity investment decisions (Jensen & Meckling, 1976; Shavell, 1984) Organizations should adopt well-structured business models characterized by customer relationship management (CRM), trust-building initiatives, research and development (R&D), and a proactive approach to avoiding cyber threats.

In the last, the discussion emphasizes the need for a holistic cybersecurity investment strategy that considers financial, strategic, legal, risk, and organizational aspects. Collaboration between cybersecurity professionals and executives is crucial to developing and implementing robust strategies that not only protect against cyber threats, but also align with the overall objectives and values of the organization. As the business landscape evolves into digital enterprises, the study suggests that executives in 2023 are expected to prioritize cybersecurity, positively influencing awareness and company strategy (Kamiya et al., 2021; Kaplan et al., 2015; Naseer et al., 2021). Ultimately, the results contribute to the ongoing dialogue on effective cybersecurity investment practices in the ASEAN region and provide insights applicable to a broader context.

6.1 Implications for Theory

The findings of this study have significant implications for theory, particularly in the context of the Resource Based View (RBV) theory. By providing empirical evidence of the factors influencing corporate cybersecurity investment in the ASEAN region, this study contributes to the advancement of RBV theory. According to RBV theory, enterprises should leverage their unique resources and competencies to gain a competitive edge (Barney, 2016; Barney, 1986). Furthermore, in the specific context of ASEAN enterprises, it is essential to consider both challenges and opportunities when making investments in cybersecurity. By integrating the RBV theory with the insights derived from this study, companies can enhance their understanding of the key elements that drive effective cybersecurity investment plans. This holistic approach can enable organizations to align their resources and capabilities with cybersecurity strategies that are tailored to their specific needs and circumstances. Furthermore, the study underscores the importance of incorporating risk management and organizational variables into decision-making processes related to cybersecurity investments. A well-defined cybersecurity strategy, coupled with careful financial considerations, is crucial for organizations seeking to improve their cybersecurity posture and resilience against evolving threats. By integrating these elements into their strategic planning, businesses can better position themselves to address cybersecurity challenges effectively and protect their valuable assets (Sukma & Leelasantitham, 2022a, 2022c, 2022d). In summary, the implications of this study for theory highlight the importance of leveraging RBV principles in the context of cybersecurity investment decisions. By emphasizing the importance of aligning resources, competencies, risk management practices, and organizational factors with cybersecurity strategies, businesses in the ASEAN region can enhance their overall cybersecurity preparedness and strategic decision-making processes.(Naseer et al., 2021)

6.2 Implications for Policy

The implications of this study extend to policymaking within ASEAN organizations and governments, highlighting the need to align corporate policies with the factors that influence cybersecurity investments. It is crucial for companies to develop robust risk assessment and risk management frameworks while fostering a culture of awareness and trust among consumers. Policymakers play a vital role in recognizing the impact of privacy laws and regulations on corporate performance and cybersecurity investment decisions(Abrahams et al., 2024; Aksoy, 2024). Additionally, governments should actively promote and support research and development initiatives that focus on addressing the increasing cyber risks faced by businesses. By integrating these insights into policy frameworks, both businesses and governments in the ASEAN region can enhance their cybersecurity resilience and readiness to combat evolving threats effectively.(Abrahams et al., 2024; Lemnitzer, 2021; Savaş & Karataş, 2022; Wilkin & Chenhall, 2020)

6.3 Implications for Innovation

In the realm of cybersecurity investment, organizations within the Association of Southeast Asian Nations (ASEAN) demonstrate a unique approach compared to their counterparts in other regions. In particular, there is a lack of emphasis on risk management and the use of insurance as a strategy to mitigate adverse outcomes. Furthermore, crucial organizational factors such as building customer trust, increasing awareness of cybersecurity risk reduction, and implementing robust cybersecurity measures are often overlooked in ASEAN entities.

Despite these identified gaps, ASEAN organizations maintain a certain level of security. However, to thrive in the rapidly evolving technological landscape, they must adapt by understanding and embracing the necessary adjustments to emerging technologies. By fostering cybersecurity innovations that enhance resilience and digital capabilities, ASEAN organizations can position themselves for global competitiveness. This strategic alignment with technological advancements will drive operational efficiency and effectiveness, ensuring that ASEAN organizations remain at the forefront of cybersecurity practices in the digital age (Aksoy, 2024; AlDaajeh et al., 2022; Kaplan et al., 2015) .

7. Conclusions

This study delves into the intricate dynamics of cybersecurity investment within the ASEAN region, employing a robust methodology that includes structural equation modeling (SEM) to analyze the relationships between key variables. The study encompassed a diverse population of companies, with a sample size that allowed for comprehensive insights into cybersecurity investment practices. By examining constructs such as cybersecurity strategy, financial considerations, institutional and regulatory environments, risk assessment, and company structure, the research sheds light on the interconnected nature of factors influencing investment decisions. In particular, the findings underscore the critical role of financial resources as the primary driver of cybersecurity investment in ASEAN, emphasizing the need for organizations to allocate adequate funds to combat evolving cyber threats. Additionally, the study highlights the significant impact of institutional and regulatory frameworks in shaping investment behavior, signaling a growing awareness of compliance with legal requirements among firms in the region. Moving beyond theoretical insights, the practical implications of this research are profound for businesses and policymakers in ASEAN. The recommendations of this study include the implementation of comprehensive cybersecurity strategies, the allocation of sufficient financial resources, the adherence to regulatory frameworks, and the cultivation of a cybersecurity-conscious organizational culture. These actions are vital to strengthening cybersecurity investments and improving resilience against cyber threats. Looking ahead, stakeholders must prioritize sustainability in cybersecurity investments by integrating risk management practices, fostering continuous education on cybersecurity best practices, and proactively addressing emerging threats. By embracing these recommendations, organizations can fortify their cybersecurity posture and protect their digital assets effectively.

In conclusion, this study not only provides valuable information on cybersecurity investment practices, but also serves as a call to action for businesses and policymakers in the ASEAN region to prioritize cybersecurity resilience. Future research directions should focus on exploring innovative cybersecurity strategies, evaluating the impact of industry-specific regulations, and quantifying the relationship between cybersecurity investments and organizational performance indicators. By fostering a culture of continuous improvement and collaboration, the ASEAN region can navigate the evolving cybersecurity landscape with confidence and resilience.

8. Limitations and further research

When conducting research on ASEAN corporate cybersecurity investment variables, it is crucial to recognize certain limitations that may impact the study's results. Firstly, the diverse range of languages within the region could pose challenges for data collection and interpretation. To address this issue, researchers can use multilingual surveys or translation services to facilitate effective communication with participants. Additionally, the varying laws and regulations among ASEAN member nations may influence cybersecurity activities, highlighting the importance of conducting a comparative legal analysis to identify and understand these differences.

Furthermore, relying solely on self-reported data from ASEAN companies may introduce bias into the results. To mitigate this potential bias, researchers should consider incorporating multiple data sources and verification methods. Furthermore, the use of cross-sectional analyzes can limit the ability to observe cybersecurity trends over time. Therefore, conducting multiyear longitudinal research can provide a more comprehensive understanding of ASEAN cybersecurity investment variables and their evolution.

In terms of future research directions, it is essential to explore the cybersecurity strategies implemented by businesses in the ASEAN region and evaluate their effectiveness in mitigating risks to enhance organizational resilience against cyber threats. Additionally, studying the impact of industry-specific regulations on cybersecurity investment decisions can offer valuable information on compliance requirements and best practices.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

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.

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.

References

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, *5*(1), 120-140.

Aksoy, C. (2024). BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, *7*(1), 96-110.

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

Anderson, R. J., & Moore, T. W. (2006). The Economics of Information Security. *Science*, *314*, 610 - 613.

Barney, J. (2016). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99-120. https://doi.org/10.1177/014920639101700108

Barney, J. B. (1986). Strategic factor markets: Expectations, luck, and business strategy. *Management Science*, *32*(10), 1231-1241.

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Q.*, *24*, 169-196.

Biernacki, P., & Waldorf, D. (1981). Snowball Sampling: Problems and Techniques of Chain Referral Sampling. *Sociological Methods & Research*, *10*, 141 - 163.

Bland, J. M., & Altman, D. G. (1997). Statistics notes: Cronbach's alpha. *BMJ*, *314*, 572.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527-544.

Cao, X. (2023). ASEAN–China Digital Economy Cooperation and Its Prospects. In *DIGITAL ECONOMY AND THE SUSTAINABLE DEVELOPMENT OF ASEAN AND CHINA* (pp. 209-228). World Scientific.

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. Academic press.

Corallo, A., Lazoi, M., & Lezzi, M. (2020a). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, *114*, 103165.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*, 297-334.

Dewett, T., & Jones, G. R. (2001). The role of information technology in the organization: a review, model, and assessment. *Journal of Management*, *27*(3), 313-346.

Erdfelder, E., Faul, F., & Buchner, A. (1996). GPOWER: A general power analysis program. *Behavior research methods, instruments, & computers*, *28*, 1-11.

Etikan, I., Musa, S. A., & Alkassim, R. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*, 1.

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior research methods*, *39*(2), 175-191.

Fleury, J.-B. (2017). Crime and Punishment (Becker 1968). In A. Marciano & G. B. Ramello (Eds.), *Encyclopedia of Law and Economics* (pp. 1-5). Springer New York. https://doi.org/10.1007/978-1-4614-7883-6_17-1

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*, 39-50.

Galbiati, R., & Vertova, P. (2014). How laws affect behavior: Obligations, incentives and cooperative behavior. *International Review of Law and Economics*, *38*, 48-57. https://doi.org/10.1016/j.irle.2014.03.001

Gordon, L. A. (2007). Incentives for improving cybersecurity in the private sector: A cost-benefit perspective. *Congressional Testimony*.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438-457.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81-85.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2013). *Multivariate data analysis: Pearson new international edition PDF eBook*. Pearson Higher Ed.

Hancock, G. R. (1997). Structural equation modeling methods of hypothesis testing of latent variable means. *Measurement and Evaluation in Counseling and Development*, *30*(2), 91-105.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

Henson, R. K. (2019). Understanding Internal Consistency Reliability Estimates: A Conceptual Primer on Coefficient Alpha. *Measurement and Evaluation in Counseling and Development*, *34*(3), 177-189. https://doi.org/10.1080/07481756.2002.12069034

Jensen, M. C., & Meckling, W. H. (1976). THEORY OF THE FIRM: MANAGERIAL BEHAVIOR, AGENCY COSTS AND OWNERSHIP STRUCTURE.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond cybersecurity: protecting your digital business*. John Wiley & Sons.

Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, *14*(3), 417-431. https://doi.org/10.1108/tg-11-2019-0112

Kline, R. B. (2023). *Principles and practice of structural equation modeling*. Guilford publications.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671. https://doi.org/10.1016/j.bushor.2021.02.022

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, *6*(2), 118-136.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6*, *9*(1-2), 3-31.

Lukavchenko, A. S. (2015). *Decision-making criteria for cybersecurity adoption*.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological methods*, *1*(2), 130.

Miyamoto, I., Holzer, T. H., & Sarkani, S. (2017). Why a counterfeit risk avoidance strategy fails. *Computers & Security*, *66*, 81-96. https://doi.org/10.1016/j.cose.2016.12.015

Mohamed Mizan, N. S., Ma'arif, M. Y., Mohd Satar, N. S., & Shahar, S. M. (2019). CNDS-cybersecurity: issues and challenges in ASEAN countries. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(1.4).

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*. https://doi.org/10.1016/j.dss.2020.113476

Pfeffer, J., & Salancik, G. R. (1978). *The External Control of Organizations: A Resource Dependence Perspective*. Harper & Row. https://books.google.co.th/books?id=9d-3AAAAIAAJ

Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Tech. LJ*, *24*, 1061.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*(1), 74-104.

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7-34.

Shavell, S. (1984). A model of the optimal use of liability and safety regulation. *The Rand Journal of Economics*, *15*(2), 271-280.

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285. https://doi.org/10.1126/science.3563507

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), 45-56.

Sukma, N., & Leelasantitham, A. (2022a). Factors affecting adoption of online community water user participation. Human Behavior and Emerging Technologies, 2022, 1-13.

Sukma, N., & Leelasantitham, A. (2022b). From conceptual model to conceptual framework: A sustainable business framework for community water supply businesses [Original Research]. *Frontiers in Environmental Science, 10.* https://doi.org/10.3389/fenvs.2022.1013153

Sukma, N., & Leelasantitham, A. (2022c). The influence and continuance intention of the E-government system: A case study of community water supply business. *Frontiers in Environmental Science, 10*, 918981.

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

Thekdi, S., & Aven, T. (2019). An integrated perspective for balancing performance and risk. *Reliability Engineering & System Safety*, *190*. https://doi.org/10.1016/j.ress.2019.106525

Tran Dai, C., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy*, *3*(2), 217-235.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: research and practice gaps. *Information Security Journal: A Global Perspective*, *17*(5-6), 207-227.

Wilkin, C. L., & Chenhall, R. H. (2020). Information Technology Governance: Reflections on the Past and Future Directions. *Journal of Information Systems*, *34*(2), 257-292.

© 2025 by the authors; licensee Growing Science, Canada. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).