STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **16**, October 2026, pp 3014–3029.
Published online in International Academic Press (www.IAPress.org)

Cybersecurity Risk Management and Organisational Performance: The Moderating Role of Cybersecurity Mitigation Strategies in Saudi Insurance Companies

Hamed Abdallah Hamed Mosa [1,*], Maizaitulaidawati Md Husin [2]

[1]*Department of Insurance and Risk Management, College of Business, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia*
[2]*Department of Business Administration, Azman Hashim International Business School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*

Abstract Cybersecurity has become a strategic enterprise risk for insurers as digital transformation increases dependence on interconnected technologies and sensitive data. This study examines the relationships between cybersecurity risks and the perceived financial and operational performance of Saudi insurance companies and tests the moderating role of cybersecurity mitigation strategies. A quantitative cross-sectional survey was conducted among 150 professionals working in risk management, information technology, cybersecurity, internal audit, and related organisational functions. The proposed model was analysed using Partial Least Squares Structural Equation Modelling with SmartPLS 4.0. The results show that cybersecurity risks are negatively associated with perceived financial performance ($\beta = -0.620$, $p < 0.001$) and perceived operational performance ($\beta = -0.580$, $p < 0.001$). Cybersecurity mitigation strategies also significantly moderate both relationships. The positive interaction effects for perceived financial performance ($\beta = 0.271$, $p < 0.001$) and perceived operational performance ($\beta = 0.298$, $p < 0.001$) indicate that stronger governance, technological controls, employee awareness, regulatory compliance, and incident-response capabilities weaken the adverse performance consequences of cybersecurity risks. The study contributes to Enterprise Risk Management and organisational resilience research by conceptualising cybersecurity mitigation strategies as integrated organisational capabilities rather than isolated technical controls. It also extends empirical cybersecurity research to the Saudi insurance sector. The findings highlight the importance of embedding cybersecurity governance, preparedness, and recovery capabilities within enterprise risk-management and business-continuity systems to support secure digital transformation.

Keywords cybersecurity risks; cybersecurity mitigation strategies; enterprise risk management; organisational resilience; perceived financial performance; perceived operational performance; insurance industry; Saudi Arabia

AMS 2010 subject classifications 62H25, 62P20, 91B30

DOI: 10.19139/soic-2310-5070-3927

1. Introduction

Digital transformation has reshaped insurance operations through cloud computing, artificial intelligence, big-data analytics, and InsurTech applications. Although these technologies improve underwriting, claims processing, customer engagement, and decision-making, they also increase exposure to data breaches, ransomware, fraud, service disruption, and third-party vulnerabilities. Cybersecurity has therefore evolved from a technical concern into an enterprise-wide strategic risk that can weaken operational continuity, financial performance, reputation,

*Correspondence to: Hamed Abdallah Hamed Mosa (Email: hmosa@imamu.edu.sa; ORCID: 0009-0006-3454-8658). Department of Insurance and Risk Management, College of Business, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia. Co-author ORCID: 0000-0002-2789-8274.

ISSN 2310-5070 (online) ISSN 2311-004X (print)
Copyright © 2026 International Academic Press

and stakeholder confidence [7, 11, 12, 23]. Recent research further emphasises that organisational cyber resilience requires integrated technical and managerial capabilities that enable firms to anticipate, withstand, recover from, and adapt to cyber incidents [10, 30]. This challenge is particularly relevant to Saudi insurance companies, whose increasing reliance on digital underwriting, automated claims systems, cloud services, and customer platforms has expanded their cyber-risk exposure. Saudi evidence indicates that security controls, managerial support, employee awareness, and business alignment strengthen organisational information-security performance [2, 4]. The institutional environment has also developed rapidly: the Insurance Authority currently regulates and supervises the insurance sector, while the National Cybersecurity Authority's Essential Cybersecurity Controls and the Saudi Central Bank's Cyber Security Framework provide important governance and control requirements for Saudi organisations and financial institutions [22, 25, 27]. These arrangements connect cybersecurity resilience with the wider objectives of financial stability, secure digital transformation, and Saudi Vision 2030 [28]. From an Enterprise Risk Management (ERM) perspective, cyber risk should be integrated into governance, strategic planning, internal control, and business-continuity processes rather than managed as an isolated information-technology problem [13, 15]. Cybersecurity mitigation strategies—including governance, technological controls, employee awareness, regulatory compliance, and incident-response capabilities—can consequently be viewed as organisational resilience capabilities. Complementing ERM, Dynamic Capability Theory explains how firms adapt these capabilities to changing threats, while the Resource-Based View considers integrated cybersecurity capabilities valuable organisational resources that protect operational continuity and competitive performance. Recent evidence nevertheless indicates that the relationship between cyber-resilience capabilities and incident outcomes remains empirically underdeveloped and may vary according to organisational and environmental conditions [10, 29]. Three gaps therefore motivate this study. First, evidence remains concentrated in developed economies, with limited research on rapidly digitalising emerging insurance markets. Second, previous studies have focused predominantly on the direct consequences of cyber risk, providing less evidence on whether integrated mitigation capabilities weaken these consequences. Third, research specifically examining these relationships in Saudi insurance companies remains scarce. Accordingly, this study examines the relationships between cybersecurity risks and the perceived financial and operational performance of Saudi insurance companies and tests the moderating role of cybersecurity mitigation strategies. It contributes by positioning mitigation strategies as organisational resilience capabilities, providing evidence from an underexamined regulatory context, and offering implications for insurers and regulators seeking to strengthen secure and sustainable digital transformation.

2. Literature Review

Digital transformation has increased insurers' reliance on cloud computing, artificial intelligence, big-data analytics, the Internet of Things, and InsurTech. Although these technologies improve underwriting, claims processing, customer engagement, and decision-making, they also expand exposure to ransomware, data breaches, fraud, and system disruption [11, 12]. Cybersecurity has consequently evolved from a technical issue into a strategic enterprise risk affecting financial stability, operational continuity, reputation, and long-term competitiveness. Successful cyberattacks can reduce firm value and increase organisational uncertainty, demonstrating the importance of integrating cybersecurity into enterprise governance and risk management [23]. This challenge is particularly relevant to insurers because they process sensitive financial, medical, actuarial, and personal data through interconnected digital platforms [7]. In Saudi Arabia, Vision 2030 has accelerated digital insurance services while increasing dependence on secure technological infrastructure. Evidence indicates that effective cybersecurity practices reduce cyberattack damage in Saudi organisations [2]. Recent research on Saudi digital insurance also confirms the growing strategic importance of security, reliability, and efficient digital service delivery [1].

2.1. Cybersecurity Risks as Strategic Enterprise Risks

Cybersecurity risks differ from conventional operational risks because they are dynamic, interconnected, and capable of spreading through cloud systems, vendors, digital supply chains, and financial infrastructures. A single incident may disrupt underwriting, claims settlement, customer services, financial reporting, and regulatory

compliance simultaneously. Cyber incidents also generate indirect consequences through litigation, regulatory penalties, customer attrition, reputational damage, and declining investor confidence [7, 12, 23].

Enterprise Risk Management therefore treats cybersecurity as an organisation-wide risk requiring systematic identification, assessment, response, and monitoring [13, 15]. Cybersecurity should be incorporated into board oversight, strategic planning, internal control, business continuity, and crisis management rather than delegated exclusively to information-technology departments. Contemporary technical research likewise demonstrates that rapidly changing threats, including previously unseen malware, require adaptive and interpretable detection mechanisms rather than reliance on static protection systems [3].

The Saudi context reinforces this enterprise-wide perspective. The cybersecurity frameworks issued by the Saudi Central Bank and the National Cybersecurity Authority emphasise governance, risk assessment, incident management, monitoring, and regulatory compliance. Nevertheless, limited empirical evidence explains how such organisational capabilities influence performance within Saudi insurance companies. This study therefore conceptualises cybersecurity as a strategic enterprise risk affecting both perceived financial and operational performance.

2.2. Cybersecurity Mitigation Strategies and Organisational Resilience

Technological controls alone are insufficient to manage increasingly sophisticated cyber threats. Effective mitigation requires an integrated combination of governance, technical protection, employee awareness, regulatory compliance, monitoring, and incident-response capabilities. These mechanisms help organisations anticipate, withstand, respond to, and recover from disruptive incidents [8, 9]. Organisational resilience refers to the ability to maintain critical activities, recover from disruptions, and adapt to changing conditions [6]. Cybersecurity governance supports resilience by clarifying responsibilities, allocating resources, coordinating organisational functions, and integrating cybersecurity into strategic decisions. Employee awareness reduces behavioural vulnerabilities, while technological controls improve threat detection and containment. Incident-response and recovery capabilities further limit operational downtime and support organisational learning after an attack [5, 8, 9]. From an ERM perspective, these mechanisms coordinate cyber risk across organisational functions. Dynamic Capability Theory explains how firms adapt and reconfigure cybersecurity resources as threats evolve, while the Resource-Based View suggests that cybersecurity knowledge, governance, technological expertise, and response routines can become valuable and difficult-to-imitate resources. Recent evidence shows that cybersecurity risk management contributes to organisational resilience, although its effectiveness varies with organisational and environmental conditions [10]. Cyber resilience should not, however, be assumed to eliminate every consequence of an incident. Tsen et al. [29] found that organisations with greater cyber resilience were less likely to report attacks, but higher resilience did not consistently reduce all post-incident outcomes. This indicates that mitigation capabilities may buffer cyber exposure without completely preventing financial, operational, or reputational losses.

Accordingly, this study treats cybersecurity mitigation strategies as an integrated organisational capability, rather than describing them as a statistically untested higher-order construct.

2.3. Cybersecurity and Organisational Performance

Cyber incidents affect perceived financial performance through recovery expenditure, legal liabilities, penalties, customer compensation, reputational losses, and reduced stakeholder confidence. Market evidence shows that successful cyberattacks can reduce firm value because investors interpret them as indicators of weak governance and increased operational uncertainty [23].

Perceived operational performance is also vulnerable because insurers depend on uninterrupted digital systems. Cyber incidents may delay underwriting and claims processing, reduce system availability, interrupt customer services, and increase recovery time and costs. Effective cybersecurity capabilities can protect business continuity, service reliability, organisational agility, and stakeholder relationships [5, 12, 16].

The effect of cyber risk is unlikely to be identical across organisations. Firms with stronger governance, employee awareness, technological controls, compliance systems, and response capabilities should be better positioned to absorb and recover from disruptions. Mitigation strategies may therefore weaken, rather than eliminate, the negative relationship between cyber exposure and organisational performance.

Evidence from emerging insurance markets remains limited, particularly regarding the simultaneous examination of perceived financial and operational performance. Existing research has generally focused on direct cyber-risk consequences or isolated security practices, providing less evidence on the moderating role of integrated mitigation capabilities.

2.4. Theoretical Contributions and Research Gaps

Four gaps motivate this study. First, much of the empirical evidence originates from developed economies, while rapidly digitalising emerging insurance markets remain underrepresented. Second, prior research has concentrated mainly on the direct consequences of cyber risks. Third, governance, employee awareness, technical controls, compliance, and incident response have frequently been examined separately rather than as an integrated mitigation capability. Finally, limited evidence explains why organisations exposed to similar cyber threats experience different financial and operational outcomes.

The study addresses these gaps by integrating ERM, Dynamic Capability Theory, and the Resource-Based View. ERM explains why cyber risk requires enterprise-wide coordination; Dynamic Capability Theory explains how mitigation resources are adapted to evolving threats; and the Resource-Based View explains how accumulated cybersecurity knowledge and routines preserve organisational value.

The study contributes by examining cybersecurity mitigation strategies as capabilities that moderate the relationships between cybersecurity risks and the perceived financial and operational performance of Saudi insurance companies. It therefore extends cybersecurity research beyond direct-effect models and provides evidence from an underexamined regulatory and insurance environment.

3. Impact of Cybersecurity Risks on Organisational Performance in the Insurance Industry

Cybersecurity risks threaten insurers' financial stability, operational continuity, reputation, and competitiveness. Because insurance operations depend on interconnected systems for underwriting, claims processing, and customer services, cyber incidents can generate response costs, legal liabilities, regulatory penalties, business interruption, and reputational damage [12, 23]. These consequences may weaken profitability, service reliability, claims efficiency, and stakeholder confidence.

From an Enterprise Risk Management perspective, cybersecurity should be managed as an organisation-wide strategic risk rather than an isolated technical issue. Integrated mitigation strategies combine governance, technological controls, employee awareness, regulatory compliance, monitoring, and incident-response capabilities. These mechanisms improve preparedness, response, recovery, and organisational learning, thereby strengthening resilience [13, 15, 31]. Recent evidence also indicates that cybersecurity risk-management maturity supports organisational resilience under technological and market turbulence [10].

Cybersecurity mitigation does not necessarily eliminate cyber incidents or all their consequences. Instead, it may reduce organisational vulnerability and help firms maintain critical operations. Tsen et al. [29] found that organisations unaffected by cyber incidents demonstrated stronger education, accountability, strategy, planning, and overall cyber resilience, although resilience did not consistently reduce every post-incident outcome. This supports examining mitigation strategies as buffering capabilities rather than assuming that they completely prevent financial and operational losses.

Despite growing research, evidence remains concentrated in developed economies and direct-effect models. Limited attention has been given to whether integrated mitigation strategies weaken the negative relationship between cybersecurity risks and organisational performance, particularly within rapidly digitalising insurance markets. Accordingly, this study examines whether cybersecurity mitigation strategies moderate the relationships between cyber risks and the perceived financial and operational performance of Saudi insurance companies.

3.1. Hypotheses Development

ERM theory suggests that greater cyber-risk exposure increases financial costs, operational disruption, regulatory exposure, and reputational damage. Accordingly, firms experiencing higher cybersecurity risks are expected to report weaker perceived financial and operational performance [12, 23].

Conversely, integrated governance, technological controls, employee awareness, compliance, and incident-response capabilities may improve organisational preparedness and recovery. Cybersecurity mitigation strategies are therefore expected to weaken the negative relationships between cyber risks and organisational performance.

H1: Cybersecurity risks are negatively related to the perceived financial performance of Saudi insurance companies.

H2: Cybersecurity risks are negatively related to the perceived operational performance of Saudi insurance companies.

H3: Cybersecurity mitigation strategies positively moderate the relationship between cybersecurity risks and perceived financial performance, such that the negative relationship becomes weaker at higher levels of mitigation.

H4: Cybersecurity mitigation strategies positively moderate the relationship between cybersecurity risks and perceived operational performance, such that the negative relationship becomes weaker at higher levels of mitigation.

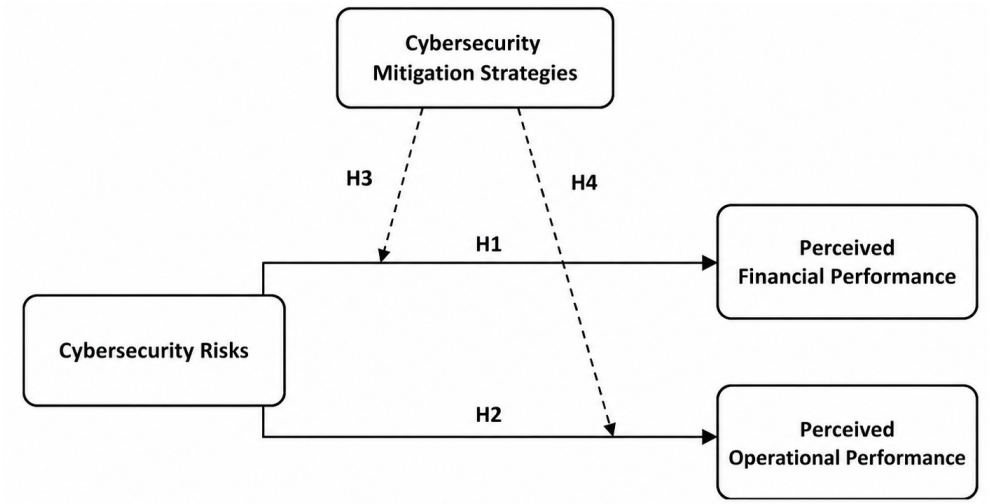

Figure 1. Proposed Research Model

Note. Solid arrows represent the direct relationships, whereas dashed arrows represent the moderating effects of cybersecurity mitigation strategies.

4. Research Methodology and Design

4.1. Research Design

This study employed a quantitative, cross-sectional design to examine the relationships between cybersecurity risks and the perceived financial and operational performance of Saudi insurance companies, together with the moderating role of cybersecurity mitigation strategies. Data were collected from professionals involved in cybersecurity, enterprise risk management, internal control, and organisational decision-making.

The model was grounded in Enterprise Risk Management, which treats cybersecurity as an organisation-wide strategic risk. Cybersecurity mitigation strategies—covering governance, technological controls, employee awareness, incident response, and regulatory compliance—were examined as organisational capabilities that may

weaken the negative relationships between cyber risks and performance. Partial Least Squares Structural Equation Modelling (PLS-SEM) in SmartPLS 4.0 was selected because the study is prediction-oriented, includes interaction effects, and does not require multivariate normality to the same extent as covariance-based SEM. The approach is therefore appropriate for estimating the proposed moderation model with a comparatively modest sample [18].

4.2. Population and Sample

The target population comprised insurance companies licensed and supervised by the Saudi Insurance Authority [22], which is currently responsible for regulating and overseeing the Saudi insurance sector. Purposive sampling was used because the study required respondents with relevant professional knowledge.

Questionnaires were distributed to professionals working in risk management, cybersecurity, information technology, internal audit, and compliance. Of 180 questionnaires distributed, 162 were returned. After excluding 12 incomplete responses, 150 valid questionnaires remained, producing an effective response rate of 83.3%. An a priori power analysis for a multiple-regression model with three predictors, a medium effect size (f^2 = 0.15), α = 0.05, and statistical power of 0.80 indicated a minimum required sample of 77 respondents. The final sample of 150 therefore exceeded the minimum requirement and was considered adequate for the estimated moderation model.

Table 1. Demographic Characteristics of Respondents (N = 150)

Characteristic	**Category**	**n**	**%**
Job position	Risk management managers	50	33.3
	IT and cybersecurity specialists	50	33.3
	Internal audit professionals	50	33.3
Insurance sector	General insurance	90	60.0
	Health insurance	20	13.3
	Takaful insurance	25	16.7
	Reinsurance	15	10.0
Experience	Less than 5 years	32	21.3
	5–10 years	58	38.7
	More than 10 years	60	40.0
Qualification	Bachelor's degree	46	30.7
	Master's degree	71	47.3
	Doctoral degree	33	22.0
Gender	Male	118	78.7
	Female	32	21.3

Table 1 shows that respondents represented major insurance activities and relevant organisational functions. Most had more than five years of experience and postgraduate qualifications, supporting their ability to assess cybersecurity practices and organisational outcomes.

4.3. Data Collection Procedure

Primary data were collected through a structured questionnaire adapted from established cybersecurity, risk-management, resilience, and organisational-performance measures. The instrument was reviewed by academic and industry experts to assess clarity, content relevance, and suitability for the Saudi insurance context.

Following minor revisions based on expert review, the questionnaire was administered once, electronically and in printed form. The primary-data component is therefore cross-sectional rather than longitudinal. Participation was voluntary, anonymous, and confidential.

4.4. Measurement of Constructs

All constructs were measured using multi-item scales and a five-point Likert scale ranging from 1, "strongly disagree", to 5, "strongly agree".

Cybersecurity Risks (CSR) captured perceived incident frequency, severity, data breaches, and operational disruption. Cybersecurity Mitigation Strategies (CMS) measured governance, technological controls, employee awareness, incident-response capability, and regulatory compliance.

Perceived Financial Performance (PFP) assessed profitability, financial stability, resource efficiency, and achievement of financial objectives. Perceived Operational Performance (POP) measured service continuity, operational efficiency, system reliability, and claims-processing effectiveness. The performance constructs were explicitly described as perceptual measures rather than audited accounting outcomes.

Table 2. Measurement Constructs and Indicator Coding

Construct	Role	Code	Measurement Indicator
Cybersecurity Risks (CSR)	Independent construct	CSR1	Frequency of cybersecurity incidents
		CSR2	Severity of cybersecurity incidents
		CSR3	Data loss resulting from cybersecurity incidents
		CSR4	Operational disruption caused by cybersecurity incidents
Cybersecurity Mitigation Strategies (CMS)	Moderating construct	CMS1	Cybersecurity governance
		CMS2	Technological security controls
		CMS3	Employee cybersecurity awareness
		CMS4	Incident-response capability
		CMS5	Regulatory compliance
Perceived Financial Performance (PFP)	Dependent construct	PFP1	Profitability relative to major competitors
		PFP2	Financial stability over the past three years
		PFP3	Financial and organisational resource efficiency
		PFP4	Financial returns relative to strategic objectives
Perceived Operational Performance (POP)	Dependent construct	POP1	Operational efficiency
		POP2	Service reliability and continuity
		POP3	Claims-processing performance
		POP4	Response to operational disruptions

Source. Adapted from Eling and Wirfs [12], Kamiya et al. [23], and Alharbi and Alsulami [2], and contextualised for the Saudi insurance sector.

Table 2 presents the four study constructs and their indicators. CSR captures perceived cyber-incident exposure, while CMS represents governance, technological, behavioural, response, and compliance capabilities. PFP and POP measure respondents' perceptions of financial and operational outcomes. All indicators were assessed on a five-point Likert scale ranging from 1, "strongly disagree", to 5, "strongly agree".

4.5. Data Analysis

The model was analysed using SmartPLS 4.0 following the two-stage procedure recommended by Hair et al. [18]. The measurement model was assessed using outer loadings, Cronbach's alpha, ρ_A, composite reliability, average variance extracted, the Fornell–Larcker criterion, HTMT, and variance inflation factors.

The structural model was evaluated using path coefficients, t-values, p-values, R^2, adjusted R^2, f^2, Q^2, model-fit indices, and interaction effects. Statistical significance was assessed using 5,000 bootstrap resamples.

4.6. Common Method Bias

Because the variables were collected from the same respondents, common method bias was examined using Harman's single-factor test and full-collinearity VIF. Procedural safeguards included respondent anonymity, clear item wording, and the separation of predictor and outcome constructs within the questionnaire.

4.7. Ethical Considerations

Participation was voluntary, and informed consent was obtained before questionnaire completion. No personally identifiable information was collected, and the responses were used solely for academic purposes. Formal ethical

approval was not required under the applicable institutional rules for anonymous, non-clinical survey research involving adult professionals.

5. Analysis and Results

5.1. Descriptive Statistics

Table 3 summarises respondents' assessments of cybersecurity risks, mitigation strategies, and perceived organisational performance. Mean scores ranged from 3.42 to 3.75. Cybersecurity Mitigation Strategies recorded the highest mean, whereas Cybersecurity Risks showed a moderate level. The standard deviations indicate adequate variation for subsequent PLS-SEM analysis.

Table 3. Descriptive Statistics of the Study Constructs

Construct	Code	Mean	SD	Minimum	Maximum
Cybersecurity Risks	CSR	3.42	0.71	1.00	5.00
Cybersecurity Mitigation Strategies	CMS	3.75	0.86	1.00	5.00
Perceived Financial Performance	PFP	3.71	0.81	1.00	5.00
Perceived Operational Performance	POP	3.74	0.79	1.00	5.00

5.2. Common Method Bias

Because all constructs were measured through a single survey, common method bias was assessed before evaluating the measurement model. Harman's single-factor test showed that the first unrotated factor explained 34.82% of the variance, below the 50% benchmark [26]. Full-collinearity VIF was 2.21, below the 3.30 threshold proposed by Kock [24]. These results suggest that common method variance was unlikely to dominate the observed relationships, although statistical tests cannot eliminate the possibility entirely.

Table 4. Common Method Bias Assessment

Assessment Method	Result	Recommended Threshold	Interpretation
Harman's Single-Factor Test	34.82%	$< 50\%$	No serious concern
Full-Collinearity VIF	2.21	< 3.30	No serious concern

Source. SPSS exploratory factor analysis and SmartPLS 4.0 output.

5.3. Measurement Model Assessment

The reflective measurement model was evaluated using indicator reliability, internal consistency, convergent validity, and discriminant validity, following established PLS-SEM guidelines [18, 17].

5.3.1. Indicator Reliability All outer loadings ranged from 0.825 to 0.914 and therefore exceeded the recommended 0.70 benchmark, supporting indicator reliability.

Table 5. Indicator Reliability (Outer Loadings)

Construct	Indicator	Outer Loading
Cybersecurity Risks (CSR)	CSR1	0.842
	CSR2	0.887
	CSR3	0.903
	CSR4	0.869
Cybersecurity Mitigation Strategies (CMS)	CMS1	0.825
	CMS2	0.874
	CMS3	0.891
	CMS4	0.904
	CMS5	0.867
Perceived Financial Performance (PFP)	PFP1	0.882
	PFP2	0.914
	PFP3	0.887
	PFP4	0.895
Perceived Operational Performance (POP)	POP1	0.863
	POP2	0.894
	POP3	0.907
	POP4	0.878

5.3.2. Internal Consistency and Convergent Validity Cronbach's alpha, ρ_A, and composite reliability exceeded 0.70 for all constructs, while AVE values ranged from 0.777 to 0.803 and exceeded 0.50. The constructs therefore demonstrated satisfactory internal consistency and convergent validity [18].

Table 6. Internal Consistency Reliability and Convergent Validity

Construct	Cronbach's α	ρ_A	CR	AVE
Cybersecurity Risks (CSR)	0.904	0.907	0.933	0.777
Cybersecurity Mitigation Strategies (CMS)	0.931	0.934	0.947	0.782
Perceived Financial Performance (PFP)	0.918	0.921	0.942	0.803
Perceived Operational Performance (POP)	0.912	0.915	0.938	0.792

Source. SmartPLS 4.0 output based on the survey data.

5.3.3. Discriminant Validity Discriminant validity was assessed using the Fornell–Larcker criterion and HTMT. The square root of each construct's AVE exceeded its correlations with other constructs, while HTMT values ranged from 0.621 to 0.836 and remained below 0.85 [14, 20]. Inspection of the cross-loading matrix also confirmed that every indicator loaded most strongly on its intended construct.

Table 7. Fornell–Larcker Criterion

Construct	CSR	CMS	PFP	POP
Cybersecurity Risks (CSR)	0.882			
Cybersecurity Mitigation Strategies (CMS)	-0.548	0.885		
Perceived Financial Performance (PFP)	-0.691	0.703	0.896	
Perceived Operational Performance (POP)	-0.654	0.742	0.781	0.890

Note. Diagonal values represent the square root of AVE; off-diagonal values are inter-construct correlations.

Table 8. Heterotrait–Monotrait Ratio (HTMT)

Construct	CSR	CMS	PFP	POP
Cybersecurity Risks (CSR)	—			
Cybersecurity Mitigation Strategies (CMS)	0.621	—		
Perceived Financial Performance (PFP)	0.781	0.744	—	
Perceived Operational Performance (POP)	0.752	0.812	0.836	—

5.3.4. Collinearity Assessment Inner VIF values ranged from 1.742 to 2.176 and were below 3.30, indicating that collinearity was not a material concern.

Table 9. Collinearity Assessment (Inner VIF)

Predictor Construct	PFP	POP
Cybersecurity Risks (CSR)	1.742	1.786
Cybersecurity Mitigation Strategies (CMS)	1.896	1.904
CSR × CMS	2.143	2.176

5.4. Structural Model Assessment

The structural model was estimated using 5,000 bootstrap resamples. Path coefficients, t-values, p-values, 95% confidence intervals, R^2, adjusted R^2, f^2, Q^2, model-fit indices, and interaction effects were evaluated in accordance with current PLS-SEM guidance [18, 19]. The reported 95% intervals use the normal approximation based on the bootstrap standard error ($\beta \pm 1.96 \times$ SEboot).

5.4.1. Hypothesis Testing Cybersecurity Risks were negatively associated with Perceived Financial Performance ($\beta = -0.620$, t = 9.874, $p < 0.001$, 95% CI $[-0.743, -0.497]$) and Perceived Operational Performance ($\beta = -0.580$, t = 8.941, $p < 0.001$, 95% CI $[-0.707, -0.453]$), supporting H1 and H2. The CSR × CMS interaction was positive for PFP ($\beta = 0.271$, t = 4.312, $p < 0.001$, 95% CI [0.148, 0.394]) and POP ($\beta = 0.298$, t = 4.815, $p < 0.001$, 95% CI [0.177, 0.419]), supporting H3 and H4. All confidence intervals excluded zero, confirming the statistical significance of the direct and moderating effects. Thus, stronger mitigation strategies weakened the negative relationships between cyber risks and perceived performance.

Table 10. Structural Path Coefficients and Hypothesis Testing

Hypothesis	Structural Path	β	t-value	p-value	95% CI	Decision
H1	CSR → PFP	-0.620	9.874	< 0.001	[-0.743, -0.497]	Supported
H2	CSR → POP	-0.580	8.941	< 0.001	[-0.707, -0.453]	Supported
H3	CSR × CMS → PFP	0.271	4.312	< 0.001	[0.148, 0.394]	Supported
H4	CSR × CMS → POP	0.298	4.815	< 0.001	[0.177, 0.419]	Supported

Note. CI = confidence interval. The 95% confidence intervals are normal-approximation bootstrap intervals computed as beta +/- 1.96 multiplied by the bootstrap standard error from 5,000 resamples. All intervals exclude zero.

5.4.2. Explanatory Power The model explained 62.4% of the variance in PFP and 65.8% in POP. The corresponding adjusted R^2 values were 0.616 and 0.651, respectively. These values indicate moderate explanatory power and show that the findings are not driven solely by the number of predictors.

Table 11. Coefficient of Determination (R-squared and Adjusted R-squared)

Endogenous Construct	R^2	**Adjusted** R^2	**Interpretation**
Perceived Financial Performance (PFP)	0.624	0.616	Moderate
Perceived Operational Performance (POP)	0.658	0.651	Moderate

Note. R-squared values of 0.75, 0.50, and 0.25 are commonly interpreted as substantial, moderate, and weak, respectively.

5.4.3. Effect Size Cybersecurity Risks had large effects on PFP ($f^2 = 0.41$) and POP ($f^2 = 0.36$). The interaction effects were medium for PFP ($f^2 = 0.18$) and POP ($f^2 = 0.21$), indicating meaningful practical moderation.

Table 12. Effect Size (f-squared)

Structural Path	f^2	**Interpretation**
CSR $\rightarrow$ PFP	0.41	Large
CSR $\rightarrow$ POP	0.36	Large
CSR $\times$ CMS $\rightarrow$ PFP	0.18	Medium
CSR $\times$ CMS $\rightarrow$ POP	0.21	Medium

5.4.4. Predictive Relevance The Q^2 values for PFP (0.462) and POP (0.488) were positive, indicating satisfactory in-sample predictive relevance. Out-of-sample predictive assessment using PLSpredict would provide an additional robustness check [17].

Table 13. Predictive Relevance (Q-squared)

Endogenous Construct	Q^2	**Interpretation**
Perceived Financial Performance (PFP)	0.462	Predictive relevance
Perceived Operational Performance (POP)	0.488	Predictive relevance

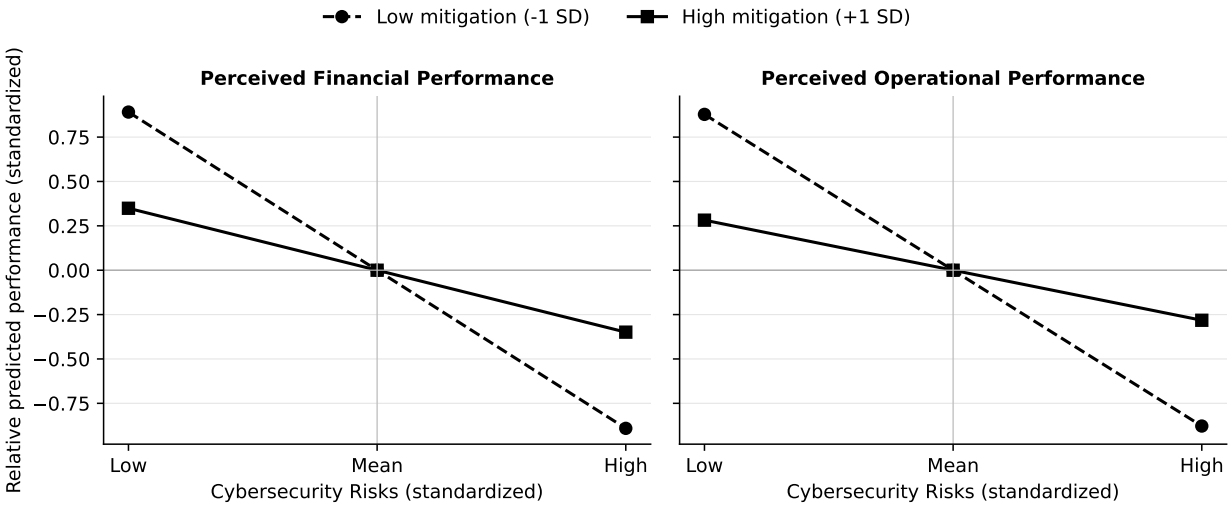

Figure 2. Conditional Effects of Cybersecurity Risks at Low and High Levels of Cybersecurity Mitigation

Note. Profiles use standardized CSR values and the reported direct and interaction coefficients. Lines are centred at zero at the mean of CSR to display differences in conditional slopes; their vertical positions are not raw Likert-scale predictions.

5.4.5. Moderation Analysis The positive interaction coefficients indicate that CMS buffers the adverse relationships between CSR and both performance dimensions. Figure 2 presents standardized conditional-slope profiles based on the reported direct and interaction coefficients. The profiles are steeper under low mitigation and flatter under high mitigation, supporting the interpretation of CMS as an organisational resilience capability.

5.4.6. Model Fit The model achieved an SRMR of 0.061, NFI of 0.921, and RMS_θ of 0.108. These values satisfy the stated thresholds and provide complementary evidence of acceptable model adequacy [21].

Table 14. Model Fit Indices

Fit Index	Obtained Value	Recommended Threshold	Assessment
SRMR	0.061	< 0.08	Good
NFI	0.921	> 0.90	Good
RMS_θ	0.108	< 0.12	Acceptable

5.5. Results Summary

Overall, the measurement model met the required reliability and validity criteria. Cybersecurity Risks were negatively related to both perceived performance dimensions, while Cybersecurity Mitigation Strategies weakened these negative relationships. The model demonstrated moderate explanatory power, meaningful effect sizes, positive predictive relevance, and acceptable fit.

6. Discussion

This study examined the relationships between cybersecurity risks and the perceived financial and operational performance of Saudi insurance companies and assessed the moderating role of cybersecurity mitigation strategies. The findings support the proposed framework: cybersecurity risks were negatively associated with both performance dimensions, while mitigation strategies weakened these negative relationships. These results reinforce the Enterprise Risk Management (ERM) perspective that cybersecurity should be managed through integrated governance and resilience mechanisms rather than isolated technical controls.

6.1. Cybersecurity Risks and Perceived Financial Performance

Cybersecurity risks were negatively related to Perceived Financial Performance, supporting H1. This finding is consistent with evidence that cyber incidents generate remediation costs, legal and regulatory liabilities, business interruption, and reputational losses [12]. Successful cyberattacks can also reduce shareholder wealth substantially, with reputational losses exceeding directly observable incident costs [23]. From an ERM perspective, these findings indicate that cyber risk can affect perceived profitability, financial stability, and resource efficiency. However, because performance was measured through respondents' perceptions, the results should not be interpreted as direct evidence of changes in audited profitability, ROA, or ROE.

6.2. Cybersecurity Risks and Perceived Operational Performance

Cybersecurity risks were also negatively related to Perceived Operational Performance, supporting H2. Cyber incidents may interrupt digital services, delay underwriting and claims processing, reduce system reliability, and increase recovery requirements. The findings therefore support the view that cybersecurity is an operational continuity issue as well as an information-security concern.

Dynamic Capability Theory suggests that organisations must continuously adapt their cybersecurity resources and procedures as threats evolve. Recent evidence similarly shows that cybersecurity risk-management maturity contributes to organisational resilience and improves firms' capacity to respond to technological and market turbulence [10].

6.3. Moderating Role of Cybersecurity Mitigation Strategies

The positive interaction coefficients support H3 and H4, indicating that cybersecurity mitigation strategies weaken the negative relationships between cybersecurity risks and both PFP and POP. Governance, technological controls, employee awareness, regulatory compliance, and incident-response capabilities therefore appear to operate collectively as organisational resilience mechanisms.

These findings extend direct-effect studies by explaining why organisations exposed to similar cyber risks may experience different outcomes. ERM explains the integration of these mechanisms across organisational functions, Dynamic Capability Theory explains their adaptation to changing threats, and the Resource-Based View positions accumulated cybersecurity knowledge and routines as valuable organisational resources.

The results should nevertheless be interpreted as buffering relationships rather than evidence that mitigation eliminates all cyber consequences. Recent research indicates that stronger cyber resilience is associated with improved organisational preparedness, although it may not reduce every post-incident outcome consistently [29].

6.4. Theoretical Implications

The study offers three theoretical contributions. First, it extends ERM by positioning cybersecurity mitigation strategies as integrated organisational capabilities rather than solely technical or compliance mechanisms. Second, it combines ERM, Dynamic Capability Theory, and the Resource-Based View to explain how mitigation capabilities weaken the negative relationships between cyber risks and perceived performance. Third, it provides evidence from the Saudi insurance industry, extending cybersecurity research to a rapidly digitalising emerging market.

6.5. Practical and Regulatory Implications

Insurance companies should integrate cybersecurity governance, technical controls, employee training, incident response, and regulatory compliance within enterprise risk-management and business-continuity systems. Boards and senior managers should also regularly assess cybersecurity maturity, clarify accountability, and test recovery capabilities.

The Insurance Authority is currently responsible for regulating and supervising the Saudi insurance sector. Regulatory coordination among the Insurance Authority, the National Cybersecurity Authority, and other relevant institutions can strengthen sector-wide cyber preparedness, operational continuity, and secure digital transformation under Saudi Vision 2030.

7. Conclusion

This study examined the relationships between cybersecurity risks and the perceived financial and operational performance of Saudi insurance companies using PLS-SEM. It also tested whether cybersecurity mitigation strategies moderate these relationships.

The results showed that cybersecurity risks were negatively associated with both PFP and POP. In contrast, the positive interaction effects indicated that stronger mitigation strategies reduced the severity of these negative relationships. Cybersecurity governance, technological controls, employee awareness, regulatory compliance, and incident-response capabilities therefore contribute to organisational resilience.

The study extends ERM by demonstrating that cybersecurity should be incorporated into governance, risk management, internal control, and business continuity. It also shows that cybersecurity capabilities may create organisational value by protecting perceived financial stability and operational continuity rather than merely satisfying regulatory requirements.

Overall, the findings position cybersecurity mitigation as an integrated organisational capability that helps Saudi insurers manage digital risk and maintain performance under increasing cyber uncertainty.

8. Limitations and Future Research

This study has several limitations. First, its cross-sectional design identifies statistical relationships but does not establish causality or capture changes in cyber resilience over time. Longitudinal and panel studies could examine how cybersecurity capabilities and performance evolve following regulatory, technological, or organisational changes.

Second, the study relies on perceptual, single-source survey measures. Although common method bias tests indicated no serious concern, future research should combine survey responses with objective indicators such as cyber-incident frequency, downtime, claims-processing time, cybersecurity expenditure, ROA, and ROE.

Third, purposive sampling and the focus on Saudi insurance companies limit statistical generalisability. Cross-country studies and comparisons involving banks, insurers, and other financial institutions could test whether regulatory and institutional conditions influence the proposed relationships.

Fourth, the model does not fully address endogeneity, firm-level clustering, or omitted organisational characteristics. Future studies should incorporate control variables such as firm size, age, digital maturity, cybersecurity budget, and board-level technological expertise.

Finally, cybersecurity mitigation strategies were examined as an integrated moderator. Future research could evaluate governance, technological controls, employee awareness, compliance, and incident response as separate dimensions or as a formally specified higher-order construct. Digital maturity, cybersecurity culture, AI-enabled security, organisational learning, and regulatory pressure could also be examined as mediators or moderators.

Declarations

Conflicts of Interest

The authors declare no conflict of interest.

Ethics Statement

The study followed recognised ethical principles for non-clinical social science research. Participation was voluntary and anonymous, and no personally identifiable information was collected. Formal institutional ethical approval was not required under the applicable guidelines for anonymous survey research involving adult professionals.

Informed Consent Statement

Informed consent was obtained from all participants before questionnaire completion.

Data Availability Statement

The anonymised data supporting the findings are available from the corresponding author upon reasonable request, subject to confidentiality and data-protection requirements.

A. Questionnaire Items

Five-point Likert scale: 1 = Strongly Disagree; 2 = Disagree; 3 = Neutral; 4 = Agree; 5 = Strongly Agree.

A1. Cybersecurity Risks (CSR)

Table 15. Cybersecurity Risks (CSR)

Code	Measurement Item
CSR1	Cybersecurity incidents occur frequently within our company.
CSR2	Cybersecurity incidents affecting our company are generally severe.
CSR3	Cybersecurity incidents have resulted in data loss or unauthorised access to sensitive information.
CSR4	Cybersecurity incidents disrupt normal business operations and service delivery.

A2. Cybersecurity Mitigation Strategies (CMS)

Table 16. Cybersecurity Mitigation Strategies (CMS)

Code	Measurement Item
CMS1	Our company has an effective cybersecurity governance framework.
CMS2	Advanced technological security controls are implemented throughout the organisation.
CMS3	Employees receive regular cybersecurity awareness and training programmes.
CMS4	Our company has effective incident-response and recovery capabilities.
CMS5	Our company complies with applicable cybersecurity regulations and standards.

A3. Perceived Financial Performance (PFP)

Table 17. Perceived Financial Performance (PFP)

Code	Measurement Item
PFP1	Our company has achieved satisfactory profitability compared with its major competitors.
PFP2	Our company has maintained stable financial performance during the past three years.
PFP3	Our company uses its financial and organisational resources efficiently.
PFP4	Our company has achieved satisfactory financial returns relative to its strategic objectives.

A4. Perceived Operational Performance (POP)

Table 18. Perceived Operational Performance (POP)

Code	Measurement Item
POP1	Our company maintains a high level of operational efficiency.
POP2	Our company provides reliable and uninterrupted insurance services.
POP3	Insurance claims are processed within established service standards.
POP4	Our company responds effectively to operational disruptions.

Note. The performance items are worded independently of cybersecurity practices to reduce conceptual overlap between the predictor and outcome constructs.

REFERENCES

1. N. Abdelrhaman, *Customer satisfaction with digital insurance services quality: Evidence from Saudi Arabia*, Statistics, Optimization & Information Computing, vol. 16, no. 2, pp. 1125–1142, 2026. https://doi.org/10.19139/soic-2310-5070-3835
2. M. Alharbi and H. Alsulami, *The impact of cybersecurity practices on cyberattack damage: A survey-based study of organizations in Saudi Arabia*, Sensors, vol. 21, no. 20, Art. 6901, 2021. https://doi.org/10.3390/s21206901

3. N. Aljarrah, H. H. Shehadeh, R. A. Obeidat, and M. Tawfik, *Cross-attention feature fusion for interpretable zero-day malware detection*, Statistics, Optimization & Information Computing, vol. 15, no. 3, pp. 2164–2178, 2026. https://doi.org/10.19139/soic-2310-5070-2900
4. A. Almuqrin, *How about enhancing organizational security: Critical success factors in information security management performance*, Journal of Global Information Management, vol. 32, no. 1, pp. 1–18, 2024. https://doi.org/10.4018/JGIM.358745
5. C. M. Angst, E. S. Block, J. D'Arcy, and K. Kelley, *When do IT security investments matter? Accounting for the influence of institutional factors in the context of data breaches*, MIS Quarterly, vol. 41, no. 3, pp. 893–916, 2017.
6. A. Annarelli and F. Nonino, *Strategic and operational management of organizational resilience: Current state of research and future directions*, Journal of Business Research, vol. 69, no. 11, pp. 4734–4743, 2016. https://doi.org/10.1016/j.jbusres.2016.04.020
7. C. Biener, M. Eling, and J. H. Wirfs, *Insurability of cyber risk: An empirical analysis*, The Geneva Papers on Risk and Insurance–Issues and Practice, vol. 40, no. 1, pp. 131–158, 2015. https://doi.org/10.1057/gpp.2014.19
8. B. Bulgurcu, H. Cavusoglu, and I. Benbasat, *Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness*, MIS Quarterly, vol. 34, no. 3, pp. 523–548, 2010.
9. J. D'Arcy, A. Hovav, and D. Galletta, *User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach*, Journal of Management Information Systems, vol. 26, no. 1, pp. 79–112, 2009.
10. S. Durst, C. Hinteregger, and M. Zieba, *The effect of environmental turbulence on cyber security risk management and organizational resilience*, Computers & Security, vol. 137, Art. 103591, 2024. https://doi.org/10.1016/j.cose.2023.103591
11. M. Eling and W. Schnell, *What do we know about cyber risk and cyber risk insurance?*, Journal of Risk Finance, vol. 17, no. 5, pp. 474–491, 2016. https://doi.org/10.1108/JRF-09-2016-0122
12. M. Eling and J. H. Wirfs, *What are the actual costs of cyber risk events?*, European Journal of Operational Research, vol. 272, no. 3, pp. 1109–1119, 2020.
13. C. Florio and G. Leoni, *Enterprise risk management and firm performance*, The British Accounting Review, vol. 49, no. 1, pp. 56–74, 2017. https://doi.org/10.1016/j.bar.2016.08.003
14. C. Fornell and D. F. Larcker, *Evaluating structural equation models with unobservable variables and measurement error*, Journal of Marketing Research, vol. 18, no. 1, pp. 39–50, 1981. https://doi.org/10.1177/002224378101800104
15. L. A. Gordon, M. P. Loeb, and L. Zhou, *Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model*, Journal of Cybersecurity, vol. 2, no. 1, pp. 31–39, 2016. https://doi.org/10.1093/cybsec/tyw004
16. V. Grover, R. H. L. Chiang, T.-P. Liang, and D. Zhang, *Building digital resilience against major shocks*, MIS Quarterly, vol. 47, no. 1, pp. 343–360, 2023.
17. J. F. Hair and A. Alamer, *Partial least squares structural equation modeling (PLS-SEM) in second language and education research: Guidelines using an applied example*, Research Methods in Applied Linguistics, vol. 1, no. 3, Art. 100027, 2022. https://doi.org/10.1016/j.rmal.2022.100027
18. J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed., SAGE, Thousand Oaks, CA, 2022.
19. J. F. Hair, M. Sarstedt, C. M. Ringle, and S. P. Gudergan, *Advanced Issues in Partial Least Squares Structural Equation Modeling*, 2nd ed., SAGE, Thousand Oaks, CA, 2023.
20. J. Henseler, C. M. Ringle, and M. Sarstedt, *A new criterion for assessing discriminant validity in variance-based structural equation modeling*, Journal of the Academy of Marketing Science, vol. 43, pp. 115–135, 2015. https://doi.org/10.1007/s11747-014-0403-8
21. J. Henseler, G. Hubona, and P. A. Ray, *Using PLS path modeling in new technology research: Updated guidelines*, Industrial Management & Data Systems, vol. 116, no. 1, pp. 2–20, 2016. https://doi.org/10.1108/IMDS-09-2015-0382
22. Insurance Authority, *About the Insurance Authority*, Government of Saudi Arabia, 2026.
23. S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, *What is the impact of successful cyberattacks on firm value?*, Journal of Financial Economics, vol. 142, no. 3, pp. 1027–1053, 2021. https://doi.org/10.1016/j.jfineco.2021.05.013
24. N. Kock, *Common method bias in PLS-SEM: A full collinearity assessment approach*, International Journal of e-Collaboration, vol. 11, no. 4, pp. 1–10, 2015. https://doi.org/10.4018/ijec.2015100101
25. National Cybersecurity Authority, *Essential Cybersecurity Controls: ECC 2-2024*, Government of Saudi Arabia, 2025.
26. P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, *Common method biases in behavioral research: A critical review of the literature and recommended remedies*, Journal of Applied Psychology, vol. 88, no. 5, pp. 879–903, 2003. https://doi.org/10.1037/0021-9010.88.5.879
27. Saudi Central Bank, *Cyber Security Framework*, Riyadh, Saudi Arabia, 2017.
28. Saudi Vision 2030, *Vision 2030: Kingdom of Saudi Arabia*, Riyadh, Saudi Arabia, 2016.
29. E. Tsen, R. K. L. Ko, and S. Slapničar, *The effect of organizational cyber resilience on cyber incident outcomes*, Journal of Cybersecurity, vol. 11, no. 1, Art. tyaf040, 2025. https://doi.org/10.1093/cybsec/tyaf040
30. V. Tzavara and S. Vassiliadis, *Tracing the evolution of cyber resilience: A historical and conceptual review*, International Journal of Information Security, vol. 23, pp. 1695–1719, 2024. https://doi.org/10.1007/s10207-023-00811-x
31. P. Yeoh, *Regulatory cyber compliance and its impact on the operational agility of insurance providers*, Journal of Financial Regulation and Compliance, vol. 28, no. 3, pp. 395–412, 2020. https://doi.org/10.1108/JFRC-01-2020-0008