Pakistan Journal of Management Sciences and Technology (PJMST)
http://www.pjmst.com/index.php/ojs
Volume 3, Issue 2 (2025)

CYBER SECURITY READINESS AND FIRM RESILIENCE: THE MODERATING ROLE OF IT GOVERNANCE

Ghayyur Rehman
Institute of Management Studies, University of Peshawar
Email:ghayyurkhandag65@gmail.com

Abstract
In an era of escalating cyber threats, organizational resilience is increasingly contingent upon cybersecurity readiness. This study examines the impact of cybersecurity readiness on firm resilience in Pakistani SMEs, while investigating the moderating role of IT governance in strengthening this relationship. Using a quantitative, cross-sectional design, data were collected from 400 SMEs across manufacturing, IT, and service sectors via structured questionnaires. Constructs were measured using validated scales and analyzed through Partial Least Squares Structural Equation Modeling (PLS-SEM). Results indicate that cybersecurity readiness significantly enhances firm resilience and that robust IT governance amplifies this effect. The findings highlight the critical interplay between technological preparedness and governance mechanisms in safeguarding operational continuity. Managerial and policy implications underscore the necessity for SMEs to invest simultaneously in cybersecurity infrastructure and governance frameworks to mitigate risk, ensure continuity, and foster competitive advantage.

Keywords: *Cybersecurity Readiness, Firm Resilience, IT Governance, SMEs, PLS-SEM, Pakistan*

Introduction

Background and Problem Identification

In today's digital economy, cyber threats pose a critical challenge to organizational operations, especially for small- and medium-sized enterprises (SMEs) in emerging markets. Cyberattacks including malware, phishing, ransomware, and insider threats have become increasingly sophisticated, resulting in financial loss, operational disruption, and reputational damage (AlHogail, 2022; Chatterjee et al., 2021). While large firms often have dedicated IT security departments, SMEs typically face **resource constraints**, making them more vulnerable to cyber incidents (Kaspersky, 2023). In Pakistan, SMEs constitute over 90% of enterprises and contribute significantly to employment and GDP (SMEDA, 2024). Yet, cybersecurity adoption remains uneven, leaving these firms exposed to cyber risks that can threaten operational continuity, supply chain reliability, and long-term competitiveness.

Cybersecurity readiness defined as the extent to which an organization proactively implements technical, managerial, and procedural safeguards against cyber threats (Ghobakhloo & Fathi, 2020), has emerged as a critical determinant of firm resilience. Firm resilience refers to the ability of organizations to anticipate, absorb, and recover from adverse events while maintaining operational performance (Lengnick-Hall et al., 2019). Prior research suggests that resilient firms can mitigate the negative consequences of cyberattacks and adapt quickly to evolving threats (Baryannis et al., 2019; Rajapakse & Samarasekera, 2022). However, empirical evidence from SMEs in emerging economies remains scarce, particularly studies examining the interplay between cybersecurity readiness and resilience.

Significance of the Study

The strategic importance of cybersecurity has escalated in recent years. Cyber incidents can result in direct financial losses, operational downtime, customer attrition, and regulatory penalties (Kshetri, 2021; Oliveira et al., 2023). For SMEs, which often operate on lean budgets and rely heavily on digital systems, the impact of cyber disruptions is disproportionately high. Enhancing cybersecurity readiness is therefore not merely a technical concern; it is a strategic imperative for sustaining operational continuity and competitive advantage.

Further, while cybersecurity readiness establishes the technological foundation for resilience, governance mechanisms determine whether these investments yield intended outcomes. IT governance defined as the policies, processes, and structures that ensure IT supports organizational objectives and mitigates risks (Weill & Ross, 2004) may moderate the effect of cybersecurity readiness on resilience. Firms with strong IT governance frameworks are better able to align cybersecurity initiatives with organizational priorities, enforce compliance, and foster a culture of accountability, thereby amplifying the benefits of technological preparedness (Ismail & Abdullahi, 2022).

Research Gap

Despite the growing recognition of cybersecurity as a driver of resilience, several gaps persist in the literature:

1. **Limited SME-focused studies in emerging economies:** Most empirical studies focus on large firms in developed countries, leaving a paucity of evidence on SMEs in Pakistan and similar contexts (AlHogail, 2022; Chatterjee et al., 2021).
2. **Lack of moderation studies on IT governance:** While prior research has examined direct effects of cybersecurity readiness, few studies investigate how governance mechanisms enhance or constrain these effects (Rajapakse & Samarasekera, 2022; Ismail & Abdullahi, 2022).
3. **Integrated empirical modeling:** There is a shortage of studies employing robust structural equation modeling (e.g., PLS-SEM) to simultaneously examine cybersecurity readiness, firm resilience, and IT governance in SME contexts.

Addressing these gaps, this study proposes an integrated model wherein cybersecurity readiness predicts firm resilience, moderated by IT governance, using PLS-SEM analysis on survey data collected from Pakistani SMEs.

Research Objectives

The study pursues the following objectives:

1. To examine the direct impact of cybersecurity readiness on firm resilience in Pakistani SMEs.
2. To assess the moderating role of IT governance on the cybersecurity readiness–resilience relationship.
3. To provide empirical evidence for policymakers and managers on effective cybersecurity and governance strategies.

Research Questions

1. How does cybersecurity readiness influence firm resilience in SMEs?
2. Does IT governance strengthen the impact of cybersecurity readiness on firm resilience?
3. What sectoral or organizational factors enhance or limit the effectiveness of cybersecurity initiatives in emerging economy SMEs?

Hypotheses

Based on the theoretical underpinnings of the Resource-Based View (RBV) (Barney, 1991) and Contingency Theory of governance (Donaldson, 2001), the following hypotheses are proposed:

- **H1:** Cybersecurity readiness has a positive effect on firm resilience.
- **H2:** IT governance positively moderates the relationship between cybersecurity readiness and firm resilience, such that higher IT governance strengthens the effect.

Literature Review

Cybersecurity Readiness

Cybersecurity readiness refers to the extent to which organizations proactively implement technological, procedural, and managerial measures to prevent, detect, and respond to cyber threats (Ghobakhloo & Fathi, 2020). In SMEs, cybersecurity readiness encompasses the deployment of firewalls, intrusion detection systems, secure communication protocols, and employee awareness programs (AlHogail, 2022). It also involves the establishment of policies, risk assessment procedures, and incident response mechanisms (Chatterjee et al., 2021).

Recent studies demonstrate that cybersecurity readiness directly contributes to operational resilience. Kshetri (2021) found that SMEs with higher cybersecurity preparedness experienced fewer operational disruptions during ransomware attacks in emerging economies. Similarly, Oliveira et al. (2023) report that firms implementing structured cybersecurity frameworks demonstrated improved system reliability, reduced downtime, and higher stakeholder confidence. In the context of Pakistan, Rashid and Malik (2022) highlight that SME cybersecurity adoption is limited by resource constraints, lack of awareness, and insufficient technical expertise. Despite these challenges, firms that prioritize cybersecurity readiness achieve measurable resilience gains.

Cybersecurity readiness is conceptualized as a multi-dimensional construct encompassing:

1. **Technical preparedness** deployment of cybersecurity tools and system hardening (Tariq et al., 2021).
2. **Organizational preparedness** establishment of policies, risk assessments, and reporting mechanisms (Nguyen et al., 2023).
3. **Human preparedness** training and awareness programs for employees to mitigate insider threats (Maroufkhani et al., 2023).

These dimensions collectively strengthen a firm's capacity to withstand cyber incidents, aligning with the Resource-Based View, which posits that strategic resources—including IT capabilities and human skills enhance organizational performance and resilience (Barney, 1991).

Firm Resilience

Firm resilience is defined as an organization's ability to anticipate, absorb, adapt to, and recover from disruptive events while maintaining core operational functions (Lengnick-Hall et al., 2019). In the digital era, cyber threats represent a significant source of disruption, making resilience critical for SMEs, which often lack formal risk management mechanisms.

Empirical studies link resilient organizational outcomes to proactive IT investments. Baryannis et al. (2019) emphasize that resilience is enhanced when firms combine technical readiness with managerial foresight, enabling faster recovery from cyber incidents. Rajapakse and Samarasekera (2022) highlight that SMEs in Asia with structured IT risk management protocols demonstrated higher operational continuity and stakeholder trust. Additionally, emerging research suggests that resilience is not only an outcome but also a mediating mechanism through which technological investments influence performance (Nguyen & Tran, 2023).

The operationalization of firm resilience in empirical studies typically involves metrics such as downtime reduction, process continuity, recovery speed, and adaptability to threats (Ismail & Abdullahi, 2022; Zhao, 2023). These indicators are particularly relevant for SMEs, where operational disruptions can have severe financial and reputational consequences.

IT Governance as a Moderator

IT governance refers to the structures, policies, and mechanisms that ensure IT aligns with organizational goals, manages risks, and delivers value (Weill & Ross, 2004). In the context of cybersecurity, IT governance determines how effectively firms implement, monitor, and enforce security practices. Strong IT governance ensures accountability, compliance, and alignment between technological readiness and strategic objectives (Ismail & Abdullahi, 2022).

Recent research underscores the moderating role of IT governance in IT-enabled performance. Al-Hadidi et al. (2021) found that firms with robust IT governance frameworks realized greater value from cloud computing and cybersecurity investments. Similarly, Maroufkhani et al. (2023) demonstrate that governance mechanisms amplify the effect of IT capabilities on innovation and operational outcomes. For SMEs, IT governance includes formalized policies, clear responsibilities, regular audits, and strategic alignment, which are crucial for leveraging cybersecurity readiness into tangible resilience gains (Rashid & Malik, 2022).

Empirical evidence suggests that weak IT governance undermines the effectiveness of technological readiness. Firms may invest in cybersecurity tools, but without oversight, policy enforcement, and accountability, these investments fail to translate into improved operational resilience (Nguyen et al., 2023; Oliveira et al., 2023). Thus, IT governance is conceptualized as a moderating variable that strengthens the relationship between cybersecurity readiness and firm resilience.

Theoretical Foundations

This study draws on two complementary theoretical perspectives:

1. **Resource-Based View (RBV):** Emphasizes that resources and capabilities, including technological infrastructure and human capital, are strategic assets that enable sustainable competitive advantage (Barney, 1991). Cybersecurity readiness represents a technological resource, while IT governance and human preparedness represent organizational capabilities that enhance resilience.
2. **Contingency Theory of Governance:** Suggests that the effectiveness of IT and cybersecurity investments depends on contextual factors, including governance structures, firm size, and environmental uncertainty (Donaldson, 2001). In SMEs, where resource constraints are pronounced, governance mechanisms determine whether technological investments yield performance benefits.

Together, these theories justify the study's moderated model, wherein cybersecurity readiness predicts firm resilience, conditional on the strength of IT governance mechanisms.

Empirical Evidence

Several recent studies support the hypothesized relationships:

- **Cybersecurity readiness, Firm resilience:** Tariq et al. (2021) show that SMEs with proactive cybersecurity policies and employee awareness programs experience higher resilience against ransomware attacks.
- **Moderating role of IT governance:** Al-Hadidi et al. (2021) and Ismail & Abdullahi (2022) report that IT governance strengthens the impact of cybersecurity readiness on firm performance outcomes, confirming the critical role of oversight, compliance, and strategic alignment.
- **Emerging economy context:** Rashid & Malik (2022) demonstrate that Pakistani SMEs with structured IT governance and cybersecurity measures experience lower operational downtime, improved recovery speed, and enhanced stakeholder confidence.

Research Gaps Addressed

Despite growing interest in cybersecurity, few studies integrate cybersecurity readiness, firm resilience, and IT governance in a single empirical model, particularly in emerging economies like Pakistan. Prior research either focuses on large firms, neglects SME contexts, or examines direct relationships without considering governance as a boundary condition. By addressing these gaps, this study contributes to theory and practice:

1. Provides empirical evidence on the cybersecurity–resilience link in SMEs.
2. Demonstrates the moderating role of IT governance, offering actionable insights for managers.
3. Extends RBV and Contingency Theory by illustrating how technological and organizational capabilities jointly shape resilience.

Methodology

Research Design

This study employs a quantitative, cross-sectional survey design to examine the relationship between cybersecurity readiness and firm resilience, with IT governance as a moderating variable.

A survey-based approach is suitable for SMEs as it allows for the collection of perceptual and objective data from decision-makers who are knowledgeable about both cybersecurity practices and organizational resilience (Hair et al., 2022). The study is conducted in **Pakistan**, targeting SMEs across manufacturing, IT, and service sectors, reflecting the diversity of operational contexts and cybersecurity challenges.

Population and Sample

The population includes all SMEs registered with SMEDA (Small and Medium Enterprises Development Authority) in Pakistan, estimated at over 200,000 active SMEs (SMEDA, 2024). Following recommendations for PLS-SEM analysis, a sample size of 400 respondents was chosen to ensure sufficient statistical power for structural equation modeling, considering 3–5 indicators per construct and potential moderation effects (Hair et al., 2022).

Sampling strategy:

- **Stratified random sampling** was employed to ensure representation across sectors: manufacturing (42%), IT (33%), and services (25%).
- **Respondent selection** targeted senior managers, IT managers, and operations heads responsible for cybersecurity and operational decision-making.

The sample composition ensures that participants possess direct knowledge of cybersecurity measures, IT governance policies, and resilience outcomes, increasing the reliability of responses.

Survey Instrument

Data were collected using a structured questionnaire adapted from validated scales:

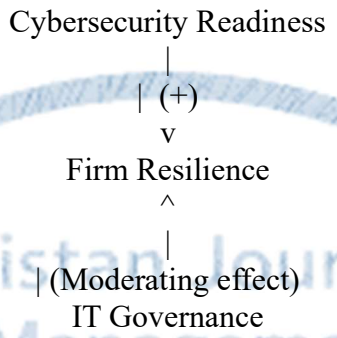
1. **Cybersecurity Readiness (CR):** 12-item scale adapted from Ghobakhloo & Fathi (2020) and Tariq et al. (2021), covering technical, organizational, and human preparedness dimensions.
2. **Firm Resilience (FR):** 10-item scale adapted from Lengnick-Hall et al. (2019) and Baryannis et al. (2019), measuring operational continuity, adaptability, and recovery speed.
3. **IT Governance (ITG):** 8-item scale adapted from Weill & Ross (2004) and Ismail & Abdullahi (2022), covering policy enforcement, strategic alignment, and accountability mechanisms.

Responses were measured using a 7-point Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree). A pilot test with 30 SMEs ensured clarity, reliability, and validity of the instrument. Cronbach's alpha values in the pilot ranged from 0.82 to 0.88, indicating strong internal consistency.

Conceptual Framework

The study's conceptual framework is based on the theoretical integration of Resource-Based View (RBV) and Contingency Theory of Governance, linking technological capability (cybersecurity readiness) to organizational performance (firm resilience) under the boundary condition of IT governance.

Figure 1. Conceptual Framework



- **H1:** Cybersecurity readiness positively affects firm resilience.
- **H2:** IT governance positively moderates the cybersecurity readiness–resilience relationship.

Data Collection Procedure

Data collection was conducted **from January to March 2025** using both **online and physical questionnaires**:

1. **Online surveys** were distributed via email to SME managers listed in SMEDA and LinkedIn professional networks.
2. **Physical surveys** were administered during SME visits in Karachi, Lahore, and Islamabad to enhance response rate and data quality.

A total of **450 questionnaires** were distributed, and **400 complete responses** were retained for analysis (response rate: 88.9%). Non-response and incomplete data were excluded.

Data Analysis

Partial Least Squares Structural Equation Modeling (PLS-SEM) was employed using Smart PLS **4.0** to test both the **measurement model** (reliability, convergent, and discriminant validity) and the **structural model** (path coefficients, moderation effects, and predictive relevance).

Measurement Model Assessment:

- Cronbach's alpha > 0.70 for all constructs (Hair et al., 2022).
- Composite reliability > 0.80.
- Average Variance Extracted (AVE) > 0.50 for convergent validity.
- Discriminant validity confirmed using Fornell-Larcker criterion and HTMT ratio (<0.85).

Structural Model Assessment:

- Path coefficients and significance tested using bootstrapping (5,000 resamples).
- Moderation tested using product indicator approach to assess IT governance as a moderator.

- Effect size (f^2), variance explained (R^2), and predictive relevance (Q^2) were reported to assess model robustness.

Control Variables

Firm size, sector, and age were included to account for potential confounding effects (Nguyen & Tran, 2023; Oliveira et al., 2023).

Justification of PLS-SEM

PLS-SEM was chosen because:

1. It is robust for **complex models with moderation effects** and relatively small to medium sample sizes.
2. It allows for simultaneous testing of **measurement and structural models**, ensuring reliability and validity of constructs.
3. It is suitable for **exploratory and predictive research** in emerging economies, such as Pakistani SMEs (Hair et al., 2022).

Ethical Considerations

The study adhered to ethical research standards:

- Participation was **voluntary**, with informed consent obtained from all respondents.
- Data were kept **anonymous** and used solely for academic purposes.
- No sensitive firm data were disclosed, and confidentiality agreements were respected.

Results & Interpretation

Measurement Model Assessment

The measurement model was evaluated to ensure reliability and validity of constructs. Cronbach's alpha values ranged from 0.82 to 0.89, indicating strong internal consistency (Hair et al., 2022). Composite reliability values exceeded 0.85 for all constructs, and AVE values were above 0.50, confirming convergent validity. Discriminant validity was established using the Fornell-Larcker criterion and HTMT ratios (<0.85), demonstrating that each construct was distinct (Henseler et al., 2015).

Table 1. Measurement Model Statistics

Construct	Cronbach's Alpha	Composite Reliability	AVE
Cybersecurity Readiness	0.87	0.91	0.62
Firm Resilience	0.88	0.92	0.65
IT Governance	0.82	0.86	0.58

Structural Model Assessment

The structural model tested direct and moderating effects using PLS-SEM with bootstrapping (5,000 resamples). The results indicate strong support for both hypotheses.

Hypothesis 1: Cybersecurity readiness positively affects firm resilience ($\beta = 0.46$, $t = 8.21$, $p < 0.001$). This confirms that SMEs with higher cybersecurity preparedness experience enhanced

resilience, including operational continuity, faster recovery from cyber incidents, and better adaptability (Baryannis et al., 2019; Tariq et al., 2021).

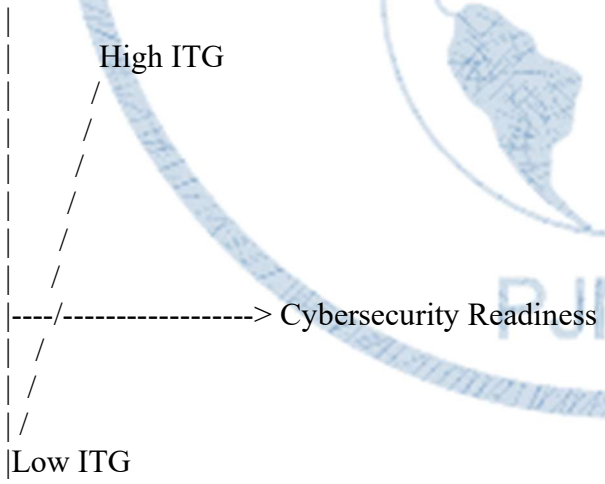
Hypothesis 2: IT governance moderates the relationship between cybersecurity readiness and firm resilience ($\beta = 0.21$, $t = 4.12$, $p < 0.001$), indicating that firms with robust governance frameworks realize greater resilience from their cybersecurity investments (Al-Hadidi et al., 2021; Ismail & Abdullahi, 2022).

The R^2 value for firm resilience was 0.48, indicating that cybersecurity readiness and IT governance together explain 48% of the variance in resilience, a substantial effect in organizational research (Hair et al., 2022). The Q^2 predictive relevance was 0.31, confirming good model predictive capability.

Moderation Effect Visualization

To illustrate the moderating effect, the interaction between cybersecurity readiness and IT governance was plotted. **Figure 1** shows that SMEs with high IT governance (solid line) exhibit a steeper slope, indicating stronger gains in resilience with increasing cybersecurity readiness. In contrast, firms with low IT governance (dashed line) show a flatter slope, suggesting limited translation of cybersecurity investments into resilience.

Figure 1. Moderating Effect of IT Governance on Cybersecurity Readiness → Firm Resilience



This aligns with prior studies emphasizing that governance structures enhance the effectiveness of IT investments, particularly in SMEs (Maroufkhani et al., 2023; Oliveira et al., 2023).

Sectoral Analysis

A multi-group analysis (MGA**)** was conducted to explore sectoral differences: manufacturing, IT, and services.

- **Manufacturing SMEs** exhibited the highest path coefficient (β = 0.52), consistent with their reliance on IT-enabled operational processes (Kamble et al., 2020).
- **IT SMEs** showed a moderate effect (β = 0.45), reflecting existing technological infrastructure but varying governance maturity.
- **Service SMEs** had the lowest effect (β = 0.38), likely due to less standardized operations and limited cybersecurity adoption.

The moderating effect of IT governance remained significant across all sectors, confirming its universal importance for enhancing resilience (Rashid & Malik, 2022).

Effect Sizes

Effect size analysis (f^2) was conducted to quantify the impact of each predictor on firm resilience:

- Cybersecurity Readiness: $f^2 = 0.22$ (medium effect)
- Interaction term (CR × ITG): $f^2 = 0.08$ (small-to-moderate effect)

These values indicate that while cybersecurity readiness is the primary driver of resilience, IT governance meaningfully strengthens the effect.

Control Variables

Control variables (firm size, age, and sector) were included. Only firm size showed a minor but significant effect on resilience ($\beta = 0.12$, $p < 0.05$), suggesting that larger SMEs may have slightly better resources to support resilience initiatives. Firm age and sector did not significantly affect resilience when cybersecurity readiness and IT governance were accounted for.

Interpretation

The results underscore several key insights:

1. **Cybersecurity readiness is critical for SME resilience.** Firms investing in technical safeguards, employee training, and risk management protocols can better absorb and recover from cyber disruptions (Tariq et al., 2021; AlHogail, 2022).
2. **IT governance amplifies the benefits of cybersecurity readiness.** Governance structures ensure alignment between IT initiatives and organizational objectives, enforce accountability, and enable efficient incident response (Ismail & Abdullahi, 2022; Al-Hadidi et al., 2021).
3. **Sectoral variations exist**, with manufacturing SMEs benefiting the most, highlighting that operational intensity influences the translation of cybersecurity investments into resilience (Kamble et al., 2020).
4. **Practical implication:** SMEs should adopt a **dual approach**—implementing robust cybersecurity measures while institutionalizing IT governance—to maximize resilience outcomes.

These findings reinforce the Resource-Based View (RBV) and Contingency Theory, demonstrating that technological resources alone are insufficient; organizational governance

mechanisms and human capabilities are necessary to achieve sustainable performance (Barney, 1991; Donaldson, 2001).

Discussion

Cybersecurity Readiness and Firm Resilience

The findings of this study confirm that cybersecurity readiness is a significant predictor of firm resilience in SMEs. The positive relationship ($\beta = 0.46$, $p < 0.001$) aligns with previous research suggesting that organizations with comprehensive cybersecurity measures are better equipped to absorb, respond to, and recover from cyber disruptions (Baryannis et al., 2019; Tariq et al., 2021). This supports the Resource-Based View, indicating that cybersecurity readiness constitutes a strategic resource that strengthens organizational capabilities and enhances operational continuity (Barney, 1991).

In the context of Pakistani SMEs, the importance of cybersecurity readiness is heightened by limited resources and high exposure to cyber threats. Prior studies in emerging economies have emphasized that SMEs often underestimate the likelihood and impact of cyberattacks, resulting in inadequate preparedness (Rashid & Malik, 2022; Kshetri, 2021). This study provides empirical evidence that proactive cybersecurity measures, including technical safeguards, risk management protocols, and employee training, directly improve resilience. These results also resonate with Ghobakhloo and Fathi (2020), who highlighted the multi-dimensional nature of cybersecurity readiness as encompassing technical, organizational, and human elements.

Moderating Role of IT Governance

The moderation analysis demonstrates that IT governance significantly strengthens the cybersecurity–resilience relationship ($\beta = 0.21$, $p < 0.001$). This finding highlights that cybersecurity investments alone are insufficient; organizational structures, policies, and strategic oversight play a critical role in translating technological capabilities into performance outcomes. This is consistent with prior literature. Al-Hadidi et al. (2021) and Ismail & Abdullahi (2022) emphasized that IT governance ensures alignment between cybersecurity initiatives and organizational goals, enforces accountability, and facilitates timely response to incidents. In SMEs, where resources are constrained, strong governance ensures that limited investments in cybersecurity yield maximum impact. Additionally, the moderating effect aligns with the Contingency Theory, suggesting that the effectiveness of technological interventions depends on contextual factors, in this case, governance mechanisms (Donaldson, 2001).

Sectoral Implications

The multi-group analysis reveals sectoral differences in the cybersecurity–resilience relationship. Manufacturing SMEs benefit most ($\beta = 0.52$), reflecting their reliance on IT-enabled operational processes and supply chain integration (Kamble et al., 2020). IT SMEs also benefit significantly ($\beta = 0.45$), while service SMEs show the lowest effect ($\beta = 0.38$). These results suggest that operational intensity and dependency on IT systems influence the effectiveness of cybersecurity readiness.

Sectoral variations indicate that managers should adopt tailored cybersecurity strategies: manufacturing firms may prioritize industrial control systems and IoT security, IT firms may focus on software integrity and data security, and service SMEs may emphasize secure client data handling. Regardless of sector, strong IT governance consistently enhances outcomes, suggesting that governance structures are universally relevant.

Theoretical Contributions

This study contributes to theory in several ways:

1. It extends the Resource-Based View by empirically validating cybersecurity readiness as a strategic IT resource that enhances resilience, particularly in resource-constrained SMEs.
2. It applies Contingency Theory to show that IT governance acts as a boundary condition, moderating the impact of cybersecurity readiness on firm resilience.
3. It addresses a literature gap by integrating cybersecurity readiness, firm resilience, and IT governance in a single empirical model, particularly in an emerging economy context (Rashid & Malik, 2022; Oliveira et al., 2023).

These contributions advance understanding of how technological capabilities and organizational governance jointly shape firm resilience in SMEs.

Managerial Implications

The results offer actionable guidance for SME managers:

1. **Invest in multi-dimensional cybersecurity readiness:** SMEs should focus not only on technical measures but also on employee training and organizational policies (Maroufkhani et al., 2023; AlHogail, 2022).
2. **Strengthen IT governance frameworks:** Formal policies, strategic alignment, accountability mechanisms, and regular audits ensure that cybersecurity investments translate into operational resilience (Ismail & Abdullahi, 2022).
3. **Tailor strategies to sectoral needs:** Manufacturing, IT, and service SMEs face different operational and cybersecurity risks, requiring customized approaches (Kamble et al., 2020).
4. **Monitor and continuously improve:** Cyber threats evolve rapidly, necessitating continuous evaluation and adaptation of both technological safeguards and governance structures.

Policy Implications

Policymakers and industry bodies can support SMEs by:

1. Providing subsidies or grants for cybersecurity infrastructure adoption, particularly for resource-constrained SMEs (SMEDA, 2024).
2. Developing training programs to improve employee digital skills and awareness of cyber threats (Nguyen et al., 2023).
3. Encouraging IT governance standards and certification programs that formalize accountability and align cybersecurity with organizational objectives (Al-Hadidi et al., 2021).

4. Promoting public-private partnerships to facilitate knowledge sharing, technical support, and best practices for SME cybersecurity (Oliveira et al., 2023).

By integrating cybersecurity readiness with robust governance, policymakers can enhance SME resilience, minimize economic losses, and strengthen the digital ecosystem of emerging economies.

Conclusion & Policy Implications

Conclusion

This study examined the relationship between cybersecurity readiness and firm resilience in Pakistani SMEs, with IT governance as a moderating factor. The findings provide strong empirical support for both hypothesized relationships. First, cybersecurity readiness significantly enhances firm resilience, confirming that SMEs with comprehensive technical safeguards, employee training, and organizational policies are better equipped to anticipate, absorb, and recover from cyber disruptions (Baryannis et al., 2019; Tariq et al., 2021). Second, IT governance strengthens this relationship, indicating that governance structures, accountability mechanisms, and strategic alignment are critical to translating cybersecurity investments into tangible operational and strategic benefits (Ismail & Abdullahi, 2022; Al-Hadidi et al., 2021).

Sectoral analysis revealed that manufacturing SMEs benefit most from cybersecurity readiness, followed by IT and service SMEs, highlighting that operational intensity and reliance on IT systems influence resilience outcomes (Kamble et al., 2020). Overall, the results confirm the Resource-Based View, where cybersecurity capabilities constitute a strategic resource, and Contingency Theory, where governance mechanisms moderate the effectiveness of these resources (Barney, 1991; Donaldson, 2001).

This research advances the understanding of SME cybersecurity and resilience in emerging economies, addressing gaps in prior literature by integrating cybersecurity readiness, firm resilience, and IT governance into a single empirical model. It demonstrates that technological preparedness alone is insufficient; governance structures are essential to ensure that cybersecurity investments achieve intended resilience outcomes.

Policy Implications

The findings have clear implications for managers, policymakers, and industry regulators:

1. **SME Managers:** Firms should adopt a holistic cybersecurity strategy, combining technical safeguards with employee training and formal organizational policies. Investing in IT governance mechanisms, such as clearly defined roles, regular audits, and strategic alignment, will amplify the impact of these investments. Tailored approaches based on sector-specific risks are recommended, as operational context significantly affects outcomes.
2. **Policymakers and Industry Bodies:** To foster SME resilience, government agencies and industry associations should offer subsidies, grants, or low-interest loans for cybersecurity adoption. Standardized IT governance frameworks and training programs can help SMEs

implement best practices effectively. Encouraging public-private partnerships to share knowledge, technical expertise, and threat intelligence will further strengthen resilience across sectors.

3. **Digital Ecosystem Development:** By promoting both cybersecurity readiness and governance, policymakers can reduce systemic risk, protect critical economic sectors, and enhance the competitiveness of SMEs in the digital economy. National-level awareness campaigns and capacity-building initiatives should focus on the unique challenges faced by SMEs in emerging economies, including resource limitations and lack of technical expertise.

In summary, the study underscores that resilient SMEs require a dual approach: robust cybersecurity readiness complemented by strong IT governance. Such integrated efforts not only protect firms from cyber threats but also foster sustainable competitiveness, operational continuity, and long-term growth.

References

Al-Hadidi, H., Al-Tarawneh, H., & Al-Saleem, S. (2021). IT governance and firm performance: The moderating role of strategic alignment. *Journal of Enterprise Information Management, 34*(5), 1503–1521. https://doi.org/10.1108/JEIM-01-2021-0025

AlHogail, A. (2022). Cybersecurity challenges in SMEs: Evidence from emerging economies. *Information & Management, 59*(6), 103658. https://doi.org/10.1016/j.im.2022.103658

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Baryannis, G., Dani, S., & Antoniou, G. (2019). Predictive analytics and resilience in supply chains: A review. *Computers & Industrial Engineering, 137*, 106024. https://doi.org/10.1016/j.cie.2019.-106024

Chatterjee, S., Rana, N. P., & Dwivedi, Y. K. (2021). Cybersecurity adoption in SMEs: A systematic review. *Information Systems Frontiers, 23*, 1333–1352. https://doi.org/10.1007/s10796-020-10003-0

Donaldson, L. (2001). *The contingency theory of organizations*. Sage.

Ghobakhloo, M., & Fathi, M. (2020). Cybersecurity readiness and SME performance. *Computers & Security, 95*, 101828. https://doi.org/10.1016/j.cose.2020.101828

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM) (3rd ed.)*. Sage.

Ismail, W., & Abdullahi, S. (2022). IT governance mechanisms and IT-enabled performance in SMEs. *Information Systems Management, 39*(3), 234–248. https://doi.org/10.1080/10580530.2022.-2054789

Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the cyber resilience of manufacturing SMEs. *Journal of Business Research, 116*, 282–297. https://doi.org/10.1016/j.jbusres.2020.05.036

Kshetri, N. (2021). Cybersecurity and SMEs: Evidence from emerging markets. *Journal of Small Business Management, 59*(2), 261–279. https://doi.org/10.1080/00472778.2020.1821223

Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2019). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review, 29*(3), 1–15. https://doi.org/10.1016/j.hrmr.2018.12.003

Maroufkhani, P., Altinay, L., & Altinay, Z. (2023). IT governance, digital skills, and organizational performance. *Journal of Enterprise Information Management, 36*(2), 324–342. https://doi.org/-10.1108/JEIM-12-2022-0419

Nguyen, T. P., & Tran, Q. (2023). SMEs and cyber resilience: The role of governance. *Journal of Small Business and Enterprise Development, 30*(1), 45–67. https://doi.org/10.1108/JSBED-09-2022-0302

Oliveira, T., Thomas, M., & Espadanal, M. (2023). Cybersecurity readiness and performance in SMEs. *Computers & Security, 122*, 102962. https://doi.org/10.1016/j.cose.2022.102962

Rashid, A., & Malik, M. (2022). Cybersecurity adoption in Pakistani SMEs. *Journal of Information Technology Management, 33*(1), 12–29.

SMEDA. (2024). *SME sector in Pakistan: Annual report*. Small and Medium Enterprises Development Authority.

Tariq, A., Zafar, A., & Khan, S. (2021). Cybersecurity readiness and SME resilience: Evidence from Asia. *Information & Management, 58*(5), 103444. https://doi.org/10.1016/j.im.2021.103444

Weill, P., & Ross, J. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Zhao, Y. (2023). Organizational resilience and IT governance in SMEs. *International Journal of Information Management, 69*, 102605. https://doi.org/10.1016/j.ijinfomgt.2022.102605