

Jurnal Ilmiah Manajemen, Ekonomi dan Bisnis
VOL 5, No. 3, Oktober 2026, pp. 174-184
p-ISSN: 2809-1655 (media cetak)
e-ISSN: 2809-1981 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JIMEB/issue/view/179
DOI: https://doi.org/10.51903/jmxcvg29

Cybersecurity Governance and Business Performance: The Mediating Roles of Digital Trust and Organizational Resilience

Didik Sofiyan Haryadi, Kapsah, Aldina Esty, Henny Kumalasari Widodo, Sri Handoko
Universitas Sains dan Teknologi Komputer
Jl. Majapahit No 605, Kota Semarang, Jawa Tengah, Indonesia
E-mail: novmamindaputri@gmail.com

KEYWORDS

Business Performance;
Cybersecurity Governance;
Digital Trust;
Organizational Resilience

ABSTRACT

Cybersecurity has become an important organizational concern as businesses increasingly depend on digital technologies and information systems. This study examines the modeled relationship between Cybersecurity Governance and Business Performance and investigates the complementary mediating roles of Digital Trust and Organizational Resilience. A quantitative PLS-SEM design was applied to a simulated dataset of 180 observations and analyzed using SmartPLS 4. The simulation was constructed to be consistent with the proposed conceptual model; therefore, the reported coefficients illustrate the behavior of the specified model rather than independently observed organizational behavior. The results show positive modeled relationships between Cybersecurity Governance and Business Performance (β = 0.201), Digital Trust (β = 0.742), and Organizational Resilience (β = 0.650). Digital Trust (β = 0.330) and Organizational Resilience (β = 0.399) also show positive modeled relationships with Business Performance. The indirect effects through Digital Trust and Organizational Resilience are 0.245 and 0.259, respectively, while the direct relationship remains significant. These results illustrate a complementary mediation pattern within the simulated model. Because the data were generated from the proposed model, the findings should be interpreted as simulation-based illustrations and not as evidence of real-world organizational effects. Empirical validation using organizational data is therefore required.

OPEN ACCESS

This journal is an open-access publication. All articles are freely and permanently accessible to everyone. Copyright ©2026 by the Author(s). This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).

ABSTRAK

Keamanan siber telah menjadi perhatian penting bagi organisasi seiring dengan meningkatnya ketergantungan bisnis pada teknologi digital dan sistem informasi. Penelitian ini menganalisis hubungan yang dimodelkan antara Cybersecurity Governance dan Business Performance serta menguji peran mediasi komplementer Digital Trust dan Organizational Resilience. Penelitian menggunakan pendekatan kuantitatif PLS-SEM pada dataset simulasi sebanyak 180 observasi yang dianalisis menggunakan SmartPLS 4. Dataset simulasi disusun agar konsisten dengan model konseptual yang diusulkan; karena itu, koefisien yang dilaporkan menggambarkan perilaku model yang ditentukan dan bukan perilaku organisasi yang diamati secara independen. Hasil menunjukkan hubungan positif yang dimodelkan antara Cybersecurity Governance dengan Business Performance (β = 0,201), Digital Trust (β = 0,742), dan Organizational Resilience (β = 0,650). Digital Trust (β = 0,330) dan Organizational Resilience (β = 0,399) juga menunjukkan hubungan positif yang dimodelkan dengan Business Performance. Pengaruh tidak langsung melalui Digital Trust dan Organizational Resilience masing-masing sebesar 0,245 dan 0,259, sedangkan hubungan langsung tetap signifikan. Hasil tersebut mengilustrasikan pola mediasi komplementer dalam model simulasi. Karena data dibangkitkan berdasarkan model yang diusulkan, temuan harus dipahami sebagai ilustrasi berbasis simulasi dan bukan sebagai bukti pengaruh pada organisasi nyata. Validasi menggunakan data empiris organisasi tetap diperlukan.

Kata Kunci: *Business Performance; Cybersecurity Governance; Digital Trust; Organizational Resilience; PLS-SEM.*

p-ISSN: 2809-1655 e-ISSN: 2809-1981

1. INTRODUCTION

The rapid adoption of digital technologies has increased organizations' dependence on digital systems and data while also exposing businesses to cybersecurity risks that can disrupt operations and reduce stakeholder confidence. Therefore, Cybersecurity Governance has become an important strategic capability for managing digital risks, protecting critical resources, and aligning cybersecurity practices with business objectives. (Rizaldi et al., 2024) demonstrate that appropriate IT governance can strengthen organizational capabilities and support successful digital transformation, highlighting the strategic importance of governance in managing technology-related risks and resources. At the same time, effective cybersecurity governance can strengthen Digital Trust, as stakeholders increasingly expect organizations to provide secure, reliable, and responsible digital services; (Safira Ardina Putri & Eskasari Putri, 2024) emphasize the importance of security and reliability in shaping trust and the acceptance of digital services.

Furthermore, strong governance can support Organizational Resilience by enabling organizations to adapt to technological changes, maintain continuity, and respond effectively to disruption. This is consistent with (Maheswari & Santoro, 2026), who found that organizational agility significantly supports business sustainability in digital startups, emphasizing the importance of adaptive organizational capabilities in dynamic digital environments. However, previous studies have generally examined governance, digital trust, organizational resilience, and business performance separately, leaving limited understanding of how cybersecurity governance contributes to business performance through these organizational mechanisms. Therefore, this study examines the relationship between Cybersecurity Governance and Business Performance by investigating the mediating roles of Digital Trust and Organizational Resilience.

The increasing dependence of businesses on digital technologies, data, and interconnected systems has made cybersecurity and digital trust important strategic concerns for organizations. Recent evidence shows that cybersecurity governance is no longer limited to protecting information systems but can also create business value by strengthening investor trust and supply-chain trust (Tan et al., 2025). At the same time, digital trust has become increasingly relevant to organizational value, as empirical evidence from US firms indicates that digital trust is associated with firm value and governance characteristics (Kluiters et al., 2023).

The growing complexity of digital risks also requires organizations to develop resilience capabilities, with (Mohammed Alharbi, 2025) emphasizing cybersecurity governance as an important foundation for organizational resilience and sustainable risk management. Furthermore, digitalization has increased the importance of responsible digital governance in building and maintaining digital trust among stakeholders (Jelovac et al., 2022). These developments indicate a shift in business practice from viewing cybersecurity as a technical protection function toward recognizing it as a strategic governance capability that can strengthen digital trust and organizational resilience and, ultimately, contribute to business performance.

From a strategic management perspective, Cybersecurity Governance represents an organizational capability for managing cybersecurity risks, protecting digital resources, and aligning security practices with business objectives. (Hasani et al., 2023) found that cybersecurity adoption positively influences organizational performance, indicating that cybersecurity capabilities can provide value beyond technical protection. Shaikh and Siponen (2024) further demonstrated that cybersecurity performance information influences subsequent cybersecurity investment decisions, highlighting the importance of managerial decision-making and organizational learning in cybersecurity management. In addition, (Smaili et al., 2022) showed that corporate governance characteristics influence cybersecurity disclosure, emphasizing the importance of governance and managerial oversight in managing cybersecurity-related issues. These findings indicate that cybersecurity governance involves not only technological protection but also organizational processes, managerial oversight, risk management, and strategic decision-making that can support organizational performance.

Digital Trust and Organizational Resilience are also important organizational capabilities in increasingly digital business environments. Digital trust refers to stakeholders' confidence in an organization's ability to manage digital technologies, information, and transactions securely and responsibly. (Launer et al., 2022)

p-ISSN: 2803-1507 e-ISSN: 2803-1531

emphasized that digital trust is an important component of digital transformation because trust supports relationships between organizations and their digital stakeholders. Meanwhile, organizational resilience refers to an organization's ability to anticipate, respond to, recover from, and adapt to disruptions. (Lin & Fan, 2024) found that organizational resilience contributes to sustainable performance, while digital technology can strengthen firms' ability to develop resilience.

(Garrido-Moreno et al., 2024) also demonstrated that organizational resilience functions as an important dynamic capability for maintaining business performance under uncertain conditions. Furthermore, (Chen et al., 2024) found that digital transformation strengthens corporate resilience by improving operational efficiency, business diversification, and organizational capabilities. Overall, these studies highlight that cybersecurity governance, digital trust, and organizational resilience are increasingly important organizational capabilities for managing digital risks, maintaining stakeholder confidence, adapting to disruption, and supporting sustainable business performance.

Despite growing research on cybersecurity, digital trust, and organizational resilience, the literature remains fragmented in explaining how cybersecurity governance can be translated into business value through more than one organizational mechanism. Digital Trust and Organizational Resilience are theoretically complementary but conceptually distinct. Digital Trust represents stakeholder confidence in the security, reliability, accountability, and responsible use of digital systems, whereas Organizational Resilience represents the organization's adaptive capacity to anticipate, respond to, recover from, and adapt to disruption. Accordingly, the two mediators explain different stages of the value-creation process: trust reflects the stakeholder-facing mechanism through which governance reduces uncertainty and supports confidence, while resilience reflects the organization-facing mechanism through which governance strengthens preparedness, continuity, recovery, and adaptation.

The novelty of the proposed framework therefore lies not simply in combining four constructs, but in distinguishing these two mechanisms within one model of how cybersecurity governance may be associated with business performance. This study aims to examine the modeled relationship between Cybersecurity Governance and Business Performance and the mediating roles of Digital Trust and Organizational Resilience. The contribution is a more differentiated explanation of the proposed mechanism, while recognizing that the simulation design does not establish empirical causality.

2. LITERATURE REVIEW

2.1 Cybersecurity Governance

Cybersecurity Governance can be understood as a strategic organizational capability because it coordinates responsibilities, oversight, risk management, and decision-making around cybersecurity rather than treating security as an isolated technical function (Slapničar et al., 2023; Yusif et al., 2024). Within a capability-based perspective, governance is valuable when organizational arrangements enable resources and managerial attention to be coordinated toward changing risk conditions and business objectives. Slapničar et al. (2023) emphasize accountability across cybersecurity functions, executives, internal audit, and boards, while Yusif et al. (2024) highlight stakeholder coordination and governance structures in managing cyber risks. These findings support viewing Cybersecurity Governance as an organizational capability that coordinates security resources and managerial action. However, because the present study uses simulated data, this theoretical positioning is tested only as a modeled relationship rather than as an empirically established capability effect.

2.2 Digital Trust

Digital Trust refers to stakeholders' confidence in an organization's ability to manage digital technologies, information, and transactions securely, reliably, and responsibly. Digital Trust is therefore primarily a stakeholder-facing mechanism: it captures confidence and reduced uncertainty regarding the organization's digital practices. (Jelovac et al., 2022) show that responsible digital practices contribute to digital trust, while Kluiters et al. (2023) link digital trust with firm value and governance characteristics. In the proposed framework, Digital Trust is distinct from Organizational Resilience because trust concerns how stakeholders

p-ISSN: 2809-1655 e-ISSN: 2809-1981

evaluate the reliability and responsibility of digital operations, whereas resilience concerns how the organization itself prepares for and responds to disruption.

2.3 Organizational Resilience

Organizational Resilience refers to an organization's ability to anticipate, respond to, recover from, and adapt to disruptions (Garrido-Moreno et al., 2024; Tzavara & Vassiliadis, 2024). It represents an organization-facing adaptive capacity rather than stakeholder confidence. Garrido-Moreno et al. (2024) demonstrate that organizational resilience can function as a dynamic capability for maintaining business performance under uncertainty, while Tzavara and Vassiliadis (2024) emphasize governance and preparedness in cyber resilience. In this framework, Organizational Resilience complements Digital Trust by explaining how cybersecurity governance may be translated into operational continuity, recovery, and adaptation after or during disruption.

2.4 Business Performance

Business Performance reflects the extent to which an organization achieves its operational and strategic objectives through outcomes such as efficiency, growth, competitiveness, and sustainability. In digital environments, performance increasingly depends on organizational capabilities that enable firms to manage technological risks and adapt to changing conditions. (Samsuden et al., 2024) show that digital capabilities can improve operational efficiency, competitiveness, and innovation, while (Garrido-Moreno et al., 2024) demonstrate the contribution of organizational resilience to business performance. Accordingly, Business Performance represents an important organizational outcome that can be supported by strategic capabilities such as Cybersecurity Governance, Digital Trust, and Organizational Resilience.

2.5 Cybersecurity Governance, Digital Trust, and Business Performance

Cybersecurity Governance can be associated with Business Performance directly because governance coordinates cybersecurity responsibilities, risk management, and managerial oversight with organizational objectives (Tan et al., 2025; Bai et al., 2024). At the same time, governance can strengthen Digital Trust by demonstrating accountability, information protection, reliable digital operations, and responsible technology management. Stakeholder confidence may then support business outcomes by reducing uncertainty and facilitating continued digital relationships. Tan et al. (2025) provide evidence that cybersecurity governance can create corporate value through investor and supply-chain trust, while Bai et al. (2024) show that trust is associated with organizational performance. These arguments support the following hypotheses:

H1: Cybersecurity Governance is positively associated with Business Performance.

H2: Cybersecurity Governance is positively associated with Digital Trust.

H4: Digital Trust is positively associated with Business Performance.

H6: Digital Trust mediates the modeled relationship between Cybersecurity Governance and Business Performance.

2.6 Cybersecurity Governance, Organizational Resilience, and Business Performance

Cybersecurity Governance can also be associated with Organizational Resilience because clear responsibilities, risk management, preparedness, and response mechanisms can strengthen an organization's capacity to cope with cyber-related disruption (Tzavara & Vassiliadis, 2024; Elsayed et al., 2024). Organizational Resilience subsequently provides an operational mechanism through which organizations may maintain continuity, recover from disruption, and adapt to changing conditions. Tzavara and Vassiliadis (2024) emphasize the governance dimension of cyber resilience, while Elsayed et al. (2024) provide evidence linking cybersecurity practices with organizational resilience and performance. This pathway is conceptually different from Digital Trust: the former concerns adaptive organizational capacity, whereas the latter concerns stakeholder confidence. These arguments support the following hypotheses:

H3: Cybersecurity Governance is positively associated with Organizational Resilience.

p-ISSN: 2803-1507 e-ISSN: 2803-1531

H5: Organizational Resilience is positively associated with Business Performance.

H7: Organizational Resilience mediates the modeled relationship between Cybersecurity Governance and Business Performance.

3. RESEARCH METHOD

3.1 Research Design

This study employs a quantitative explanatory research design to examine the modeled relationships among Cybersecurity Governance, Digital Trust, Organizational Resilience, and Business Performance. Cybersecurity Governance is positioned as the independent variable, Digital Trust and Organizational Resilience as mediating variables, and Business Performance as the dependent variable. The proposed relationships are examined using Partial Least Squares Structural Equation Modeling (PLS-SEM) (Hair & Alamer, 2022; Ringle et al., 2023). PLS-SEM is used to evaluate direct and indirect relationships among the latent constructs. Because the study uses simulated observations generated in accordance with the proposed model, the analysis is intended to demonstrate and examine the behavior of the specified structural model; it should not be interpreted as empirical evidence of organizational causality or as independently observed predictive performance.

3.2 Population and Sample

The study uses a simulated dataset of 180 observations representing hypothetical organizational members with knowledge of cybersecurity, digital operations, risk management, and business activities. The dataset was generated from predefined construct characteristics and the proposed structural model rather than collected from actual participants. The simulation used the four constructs in the specified order—Cybersecurity Governance, Digital Trust, Organizational Resilience, and Business Performance—and indicator responses were represented on a five-point Likert scale (Amusa & Hossana, 2024; Sturman, 2025). Importantly, the original dataset documentation available for this manuscript does not retain a verifiable record of the software or AI generator, random seed, exact distribution parameters, or correlation matrix used during the initial data-generation step. To avoid inventing undocumented settings, this revision does not assign a software package, seed, or distributional parameter retrospectively.

The reproducible elements that can be verified from the manuscript are the sample size (n = 180), construct definitions, five-point response scale, proposed path structure, and SmartPLS 4 as the analysis software. The dataset was constructed to be consistent with the proposed relationships; therefore, the resulting significant coefficients, R^2 values, and mediation effects are partly consequences of the simulation assumptions and cannot be treated as independently observed organizational relationships. Before empirical submission, the complete original generation script or generation log should be retained as supplementary material so that the exact generator, seed, distributional assumptions, and randomization procedure can be independently reproduced.

3.3 Research Instrument and Measurement

The measurement dimensions were adapted from the supporting literature and contextualized for cybersecurity and digital business. Because the original simulation record does not preserve a verbatim item-level mapping to the source scales, the indicators in Table 1 should be understood as contextualized indicator statements derived from the reported dimensions rather than as direct quotations from validated questionnaires. Each indicator was represented using a five-point Likert-scale format, ranging from 1 = strongly disagree to 5 = strongly agree. For transparency, the construct dimensions and their supporting sources are retained in Table 1, while the exact wording used to generate each simulated indicator should be archived together with the dataset and generation script. This distinction is important because measurement validity in the simulated model does not establish that the same items would demonstrate equivalent validity in an empirical organizational sample.

p-ISSN: 2809-1655 e-ISSN: 2809-1981

The selected indicators capture the main dimensions of each construct and provide a consistent basis for the simulated analysis. However, the available simulation record does not preserve a complete item-level mapping to validated source scales. Accordingly, the indicators should be treated as contextualized operationalizations of the stated dimensions rather than as verbatim reproductions of validated questionnaire items. For empirical replication, each item should be linked to its original source and its adaptation procedure documented before data collection.

Table 1. Measurement of Research Variables

Construct	Operational Definition	Indicators	Supporting Reference
Cybersecurity Governance (CG)	Organizational mechanisms for directing, overseeing, and managing cybersecurity in alignment with organizational objectives.	Cybersecurity policies; management oversight; accountability; cybersecurity risk management; integration into decision-making.	(Slapničar et al., 2023)
Digital Trust (DT)	Stakeholders' confidence in the security, reliability, accountability, and responsible management of digital technologies and information.	Digital security; system reliability; information protection; responsible technology use; digital accountability.	(Saveljeva & Volkova, 2025)
Organizational Resilience (OR)	The capability to anticipate, respond to, recover from, and adapt to organizational disruptions.	Disruption readiness; response capability; operational continuity; recovery capability; adaptability.	(Baghersad & Zobel, 2022)
Business Performance (BP)	The extent to which an organization achieves its operational and strategic objectives through financial and non-financial outcomes.	Operational efficiency; process performance; competitiveness; business growth; achievement of business objectives.	(Thi Thanh Thuy et al., 2023)

3.4 PLS-SEM Analysis

The simulated dataset was analyzed using SmartPLS 4 through PLS-SEM. The analysis consisted of measurement-model and structural-model assessment. The measurement model was evaluated using outer loadings, Cronbach's Alpha, rho_A, Composite Reliability (CR), Average Variance Extracted (AVE), and the Heterotrait–Monotrait (HTMT) ratio. The structural model was assessed using path coefficients (β), R^2, and adjusted R^2, while hypothesis significance was examined using bootstrapping with 10,000 subsamples based on t-values, p-values, and 95% confidence intervals. The original analysis record does not contain verifiable Q^2 or f^2 outputs. Therefore, this revision does not introduce unsupported Q^2 or f^2 values; instead, the methodological claim is limited to explanatory assessment based on R^2 and adjusted R^2. Mediation analysis examined the indirect relationships of Cybersecurity Governance with Business Performance through Digital Trust and Organizational Resilience. An indirect effect was considered significant when its 95% bootstrap confidence interval did not include zero.

3.5 Hypothesis Testing

The hypotheses are developed based on the proposed relationships among Cybersecurity Governance, Digital Trust, Organizational Resilience, and Business Performance. The model includes five direct relationships and two indirect relationships through the mediating variables. The proposed hypotheses are summarized in Table 2.

Table 2. Research Hypotheses

Hypothesis	Proposed Relationship	Expected Effect
H1	Cybersecurity Governance → Business Performance	Positive
H2	Cybersecurity Governance → Digital Trust	Positive
H3	Cybersecurity Governance → Organizational Resilience	Positive
H4	Digital Trust → Business Performance	Positive
H5	Organizational Resilience → Business Performance	Positive
H6	Cybersecurity Governance → Digital Trust → Business Performance	Positive
H7	Cybersecurity Governance → Organizational Resilience → Business Performance	Positive

p-ISSN: 2803-1507 e-ISSN: 2803-1531

The hypotheses are tested using PLS-SEM bootstrapping. Direct effects are evaluated using the path coefficient (β), t-value, p-value, and 95% bootstrap confidence interval. The mediation hypotheses are assessed based on the significance of the indirect effects and their confidence intervals. A hypothesis is considered supported when the estimated effect is significant and the corresponding confidence interval does not include zero.

3.6 Mediation Analysis

Mediation analysis is conducted to examine whether Digital Trust and Organizational Resilience mediate the relationship between Cybersecurity Governance and Business Performance. Two indirect effects are tested: Cybersecurity Governance → Digital Trust → Business Performance and Cybersecurity Governance → Organizational Resilience → Business Performance. The mediation effects are assessed using bootstrapping based on the indirect-effect coefficient, t-value, p-value, and 95% bootstrap confidence interval. An indirect effect is considered statistically significant when its confidence interval does not include zero. The direct and total effects are also examined to determine whether the mediation is complementary, indirect-only, or unsupported.

4. RESULTS AND DISCUSSION

4.1 Measurement Model Assessment

The measurement model was assessed using SmartPLS 4 to evaluate the reliability and convergent validity of Cybersecurity Governance (CG), Digital Trust (DT), Organizational Resilience (OR), and Business Performance (BP). The assessment included outer loadings, Cronbach's Alpha, rho_A, Composite Reliability (CR), and Average Variance Extracted (AVE), based on the criteria specified in the research method. The results of the measurement model assessment are presented in Table 3.

Table 3. Measurement Model Results

Construct	Outer Loading Range	Cronbach's Alpha	rho_A	Composite Reliability	AVE
Cybersecurity Governance	0.748–0.876	0.884	0.889	0.915	0.683
Digital Trust	0.756–0.884	0.891	0.897	0.919	0.696
Organizational Resilience	0.731–0.872	0.872	0.879	0.906	0.658
Business Performance	0.743–0.881	0.887	0.893	0.917	0.690

As shown in Table 3, all indicators have outer loadings above 0.70, while Cronbach's Alpha, rho_A, and Composite Reliability values exceed 0.70 for all constructs. The AVE values also exceed 0.50, ranging from 0.658 to 0.696. These results indicate that all constructs meet the required reliability and convergent validity criteria and are adequate for further structural model assessment.

4.2 Discriminant Validity

Discriminant validity was assessed using the Heterotrait–Monotrait (HTMT) ratio to determine whether the four constructs are empirically distinct. HTMT values below 0.90 indicate adequate discriminant validity. The HTMT results are presented in Table 4.

Table 4. HTMT Results

Construct	CG	DT	OR	BP
Cybersecurity Governance (CG)	—	0.781	0.746	0.728
Digital Trust (DT)	0.781	—	0.793	0.816
Organizational Resilience (OR)	0.746	0.793	—	0.824
Business Performance (BP)	0.728	0.816	0.824	—

As shown in Table 4, all HTMT values are below 0.90, ranging from 0.728 to 0.824. This indicates that Cybersecurity Governance, Digital Trust, Organizational Resilience, and Business Performance are empirically distinct constructs. Therefore, the measurement model demonstrates adequate discriminant validity and is suitable for subsequent structural model assessment.

p-ISSN: 2809-1655 e-ISSN: 2809-1981

4.3 Structural Model Assessment

After establishing the reliability and validity of the measurement model, the structural model was assessed to evaluate the explanatory variance of the endogenous constructs. The assessment focused on R^2 and adjusted R^2 for Digital Trust, Organizational Resilience, and Business Performance. These measures describe the proportion of variance reproduced by the specified simulated relationships. Q^2 and f^2 are not reported because verifiable output values for these measures are not available in the current simulation record. Accordingly, the structural results should be interpreted as model-based explanatory illustrations rather than evidence of predictive performance in actual organizations.

Table 5. R^2 and Adjusted R^2

Endogenous Construct	R^2	Adjusted R^2
Digital Trust	0.551	0.549
Organizational Resilience	0.423	0.420
Business Performance	0.641	0.635

The simulated model explains 55.1% of the variance in Digital Trust, 42.3% of the variance in Organizational Resilience, and 64.1% of the variance in Business Performance. The adjusted R^2 values are 0.549, 0.420, and 0.635, respectively. These values indicate the explanatory behavior of the specified simulation structure. They should not be interpreted as estimates of the proportion of organizational performance that Cybersecurity Governance, Digital Trust, and Organizational Resilience would explain in a real-world population.

4.4 Direct Effect and Hypothesis Testing

Hypothesis testing was conducted using bootstrapping with 10,000 subsamples. The assessment was based on the path coefficient (β), t-value, p-value, and 95% confidence interval, consistent with the procedure specified in the research method. The direct effect results are presented in Table 6.

Table 6. Direct Effect and Hypothesis Testing

Hypothesis	Relationship	β	t-value	p-value	95% CI	Decision
H1	CG → BP	0.201	3.184	0.001	0.078–0.323	Supported
H2	CG → DT	0.742	17.436	<0.001	0.656–0.824	Supported
H3	CG → OR	0.650	11.982	<0.001	0.541–0.754	Supported
H4	DT → BP	0.330	4.876	<0.001	0.196–0.463	Supported
H5	OR → BP	0.399	5.931	<0.001	0.267–0.529	Supported

As shown in Table 6, all five modeled direct relationships are positive and statistically significant within the simulated dataset, with 95% confidence intervals excluding zero. Therefore, H1–H5 are supported as simulation-based model tests. These results should not be read as independent empirical evidence because the dataset was generated to be consistent with the proposed conceptual structure.

H1 indicates a positive modeled relationship between Cybersecurity Governance and Business Performance ($\beta = 0.201$, $p = 0.001$). H2 shows a strong positive modeled relationship between Cybersecurity Governance and Digital Trust ($\beta = 0.742$, $p < 0.001$), while H3 shows a positive modeled relationship with Organizational Resilience ($\beta = 0.650$, $p < 0.001$). These coefficients illustrate the relationships embedded in or produced by the simulation design; they do not establish that stronger governance causes greater trust or resilience in actual organizations.

H4 shows a positive modeled relationship between Digital Trust and Business Performance ($\beta = 0.330$, $p < 0.001$), while H5 shows a positive modeled relationship between Organizational Resilience and Business Performance ($\beta = 0.399$, $p < 0.001$). The two pathways represent different mechanisms: Digital Trust captures stakeholder confidence in digital security and responsible technology management, whereas Organizational Resilience captures the organization's capacity to maintain continuity, recover, and adapt. Within the simulated dataset, both mechanisms are therefore consistent with the proposed framework.

p-ISSN: 2803-1507 e-ISSN: 2803-1531

4.5 Mediation Analysis

Mediation analysis was conducted to examine whether Digital Trust and Organizational Resilience mediate the relationship between Cybersecurity Governance and Business Performance. Two indirect effects were tested using bootstrapping with 10,000 subsamples. An indirect effect is considered significant when its 95% confidence interval does not include zero. The mediation results are presented in Table 7.

Table 7. Mediation Analysis

Hypothesis	Indirect Relationship	Indirect Effect (β)	t-value	p-value	95% CI	Decision
H6	CG → DT → BP	0.245	4.691	<0.001	0.146–0.349	Supported
H7	CG → OR → BP	0.259	5.021	<0.001	0.158–0.361	Supported

As shown in Table 7, both indirect effects are positive and statistically significant within the simulated dataset, with 95% confidence intervals excluding zero. H6 is supported for the Digital Trust pathway ($\beta = 0.245$, $p < 0.001$), and H7 is supported for the Organizational Resilience pathway ($\beta = 0.259$, $p < 0.001$). Because the dataset was generated according to the proposed model, these significant indirect effects should be interpreted as illustrations of the specified mediation structure rather than independently observed mediation in organizations.

The direct modeled relationship between Cybersecurity Governance and Business Performance remains positive and significant ($\beta = 0.201$, $p = 0.001$), while both indirect pathways are also significant. Within the simulated model, this pattern is consistent with complementary mediation. The indirect effect through Organizational Resilience (0.259) is slightly larger than the Digital Trust indirect effect (0.245), a difference of 0.014. Because both values originate from the same simulation design, this small difference should not be interpreted as evidence that resilience is empirically more important than trust. At most, it illustrates that the specified simulation assigns a slightly larger modeled pathway through organizational adaptive capacity than through stakeholder confidence.

4.6 Discussion

The findings illustrate how Cybersecurity Governance can be conceptualized as a strategic organizational capability rather than only a technical control function. Within a capability-based perspective, governance coordinates accountability, risk management, oversight, and decision-making so that cybersecurity resources can be aligned with organizational objectives. However, the positive coefficients reported here are modeled associations generated within a simulated dataset and therefore cannot independently establish that governance produces better business outcomes. The result is consistent with the theoretical argument in (Hasani et al., 2023; Tan et al., 2025; Jelovac et al., 2022; Tzavara & Vassiliadis, 2024), but empirical organizational data are required to validate the proposed capability mechanism.

Digital Trust and Organizational Resilience represent complementary but distinct mechanisms. Digital Trust is stakeholder-facing: it reflects confidence in the security, reliability, accountability, and responsible use of digital systems. Organizational Resilience is organization-facing: it reflects preparedness, continuity, recovery, and adaptation when disruption occurs. Within the simulated model, both mechanisms are positively associated with Business Performance, consistent with the theoretical arguments and prior findings cited in the manuscript (Garrido-Moreno et al., 2024; Kluiters et al., 2023). The distinction is important because the two mediators should not be treated as interchangeable organizational capabilities.

The mediation results provide the main theoretical illustration of the study. Both Digital Trust and Organizational Resilience transmit part of the modeled relationship between Cybersecurity Governance and Business Performance, while the direct path remains significant. The two indirect effects are close in magnitude, with Organizational Resilience (0.259) exceeding Digital Trust (0.245) by 0.014. This small difference does not justify a substantive ranking of the mechanisms because the values are produced by the same simulated model. Instead, the result illustrates that cybersecurity governance may be theorized as having both a stakeholder-confidence pathway and an organizational-adaptation pathway. Practical implications

p-ISSN: 2809-1655 e-ISSN: 2809-1981

should therefore be treated as preliminary propositions for empirical testing rather than validated prescriptions for actual organizations.

5. CONCLUSION AND RECOMMENDATIONS

This study illustrates a proposed framework linking Cybersecurity Governance with Business Performance through Digital Trust and Organizational Resilience. Within the simulated dataset, all seven hypotheses receive statistical support, and the two mediators form complementary modeled pathways. Digital Trust represents the stakeholder-confidence mechanism, whereas Organizational Resilience represents the organizational-adaptation mechanism. These distinctions sharpen the theoretical contribution beyond simply combining four constructs in one model. However, because the observations were simulated according to the proposed model, the coefficients, significance levels, R^2 values, and mediation effects should be interpreted as illustrations of the specified model rather than empirical evidence of actual organizational effects. Accordingly, the managerial implications are preliminary: organizations may consider the potential relevance of governance, trust, and resilience together, but such recommendations require validation using actual organizational data. Future research should use empirical samples and preserve complete item-level measurement sources and data-generation or data-collection documentation so that the proposed relationships can be independently tested.

Future research should validate the proposed model using empirical data collected from organizations implementing cybersecurity governance and digital technologies. Further studies may examine the model across different industries, organizational sizes, and geographical contexts to improve the generalizability of the findings. Future research could also incorporate additional factors, such as digital capability, strategic alignment, or innovation capability, to provide a broader understanding of how cybersecurity governance contributes to business performance. Such research would strengthen the empirical validation of the model and further clarify the roles of Digital Trust and Organizational Resilience in translating cybersecurity governance into business outcomes.

REFERENCES

Amusa, B., & Hossana, T. (2024). An empirical comparison of some missing data treatments in PLS-SEM. *PLOS ONE*, *19*(1), e0297037. https://doi.org/10.1371/0297037

Baghersad, M., & Zobel, C. W. (2022). Organizational Resilience to Disruption Risks: Developing Metrics and Testing Effectiveness of Operational Strategies. *Risk Analysis*, *42*(3), 561–579. https://doi.org/10.1111/13769

Bai, J., Su, J., Xin, Z., & Wang, C. (2024). Calculative trust, relational trust, and organizational performance: A meta-analytic structural equation modeling approach. *Journal of Business Research*, *172*, 114435. https://doi.org/10.1016/2023.114435

Chen, Y., Cai, Q., Wang, Z., & Xu, Z. (2024). Has digital transformation enhanced the corporate resilience in the face of COVID-19? Evidence from China. *International Review of Financial Analysis*, *96*, 103709. https://doi.org/10.1016/2024.103709

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal 2024 10:1*, *10*(1), 115-. https://doi.org/10.1186/S43093-024-00402-9

Garrido-Moreno, A., Martín-Rojas, R., & García-Morales, V. J. (2024). The key role of innovation and organizational resilience in improving business performance: A mixed-methods approach. *International Journal of Information Management*, *77*, 102777. https://doi.org/10.1016/2024.102777

p-ISSN: 2803-1507 e-ISSN: 2803-1531

Hair, J., & Alamer, A. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research Methods in Applied Linguistics*, *1*(3), 100027. https://doi.org/10.1016/2022.100027

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *Sn Business & Economics*, *3*(5), 97. https://doi.org/10.1007/S43546-023-00477-6

Jelovac, D., Ljubojević, Č., & Ljubojević, L. (2022). HPC in business: the impact of corporate digital responsibility on building digital trust and responsible corporate digital governance. *Digital Policy, Regulation and Governance*, *24*(6), 485–497. https://doi.org/10.1108/11-2020-0164

Kluiters, L., Srivastava, M., & Tyll, L. (2023). The impact of digital trust on firm value and governance: an empirical investigation of US firms. *Society and Business Review*, *18*(1), 71–103. https://doi.org/10.1108/07-2021-0119

Launer, M., Çetin, F., & Paliszkiewicz, J. (2022). Digital trust in the workplace: Testing a new instrument on a multicultural sample. *Forum Scientiae Oeconomia*, *10*(1), 30–47. https://doi.org/10.23762

Lin, J., & Fan, Y. (2024). Seeking sustainable performance through organizational resilience: Examining the role of supply chain integration and digital technology usage. *Technological Forecasting and Social Change*, *198*, 123026. https://doi.org/10.1016/2023.123026

Maheswari, N. R., & Santoro, A. P. (2026). Organizational Agility as the Key to Business Sustainability: An Empirical Study on Digital Startups. *Jurnal Ilmiah Manajemen, Ekonomi Dan Bisnis*, *5*(1), 01–11. https://doi.org/10.51903/064

Mohammed Alharbi, T. S. (2025). Cybersecurity governance and organizational resilience: A framework for sustainable risk management. *EDPACS*. https://doi.org/10.1080/07366981.2025.2596943

Ringle, C. M., Sarstedt, M., Sinkovics, N., & Sinkovics, R. R. (2023). A perspective on using partial least squares structural equation modelling in data articles. *Data in Brief*, *48*, 109074. https://doi.org/10.1016/2023.109074

Rizaldi, M. A., Mulyana, R., & Ramadani, L. (2024). Digital Transformation of BPRACo by Designing IT Governance with COBIT 2019 SME Focus Area. *Kompak :Jurnal Ilmiah Komputerisasi Akuntansi* , *17*(2), 349–365. https://doi.org/10.51903/V17I2.2072

Safira Ardina Putri, & Eskasari Putri. (2024). Analisis Tingkat Keamanan, Fleksibilitas, Kepuasan Pengguna, Citra Sosial dan Kenyamanan Pengguna Terhadap Manfaat Bank Digital Dalam Sistem Pembayaran : Studi Kasus di Kota Surakarta. *Kompak :Jurnal Ilmiah Komputerisasi Akuntansi* , *17*(2), 460–479. https://doi.org/10.51903/17I2.2191

Samsuden, N. S., Kohar, U. H. A., Khatib, S. F. A., & Abbas, A. F. (2024). Digital Capabilities and Business Performance: A Systematic Literature Review. *Sustainability 2024, Vol. 16, Page 11108*, *16*(24), 11108. https://doi.org/10.3390/162411108

Saveljeva, J., & Volkova, T. (2025). A Survey on Digital Trust: Towards a Validated Definition. *Digital 2025, Vol. 5, Page 14*, *5*(2), 14. https://doi.org/10.3390/5020014

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems*, *51*, 100642. https://doi.org/10.1016/2023.100642

Smaili, N., Radu, C., & Khalili, A. (2022). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance 2022 27:4*, *27*(4), 1049–1071. https://doi.org/10.1007/S10997-022-09637-6

p-ISSN: 2809-1655 e-ISSN: 2809-1981

Sturman, M. C. (2025). Real Research with Fake Data: A Tutorial on Conducting Computer Simulation for Research and Teaching. *Organizational Research Methods*, *28*(1), 76–113. https://doi.org/10.1177/10944281231215024

Tan, W., Guo, B., & Zhang, Q. (2025). Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. *Pacific-Basin Finance Journal*, *90*, 102646. https://doi.org/10.1016/2024.102646

Thi Thanh Thuy, V. A., Thi Hong Nhung, P. B., Thi Tu Oanh, L. C., & Thi Kim Hoa, N. D. (2023). Factors Affecting Business Performance: Expanding Theoretical Measurements. *International Journal of Professional Business Review*, *8*(5), e02134. https://doi.org/10.26668/2023.v8i5.2134

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security 2024 23:3*, *23*(3), 1695–1719. https://doi.org/10.1007/S10207-023-00811

Yusif, S., Hafeez-Baig, A., & Anachanser, C. (2024). Internet governance and cyber-security: a systematic literature review. *Information Security Journal: A Global Perspective*, *33*(2), 158–171. https://doi.org/10.1080/19393555.2023.2268608