INKUBIS: Jurnal Ekonomi dan Bisnis
Volume 8, Issue 1, 88-100
e_ISSN: 2775-3913
https://inkubis.polteksci.ac.id/index.php/ink/index
DOI: doi.org/10.59261/inkubis.v8i1.149

Digital Risk Culture and Cyber Resilience Advantage in Indonesian Data Center Providers: Firm Competitive Performance and the Moderating Effect of Organizational Risk Response Habit

Aditya Dyan Permadi* Universitas Ciputra, Indonesia
Trianggoro Wiradinata Universitas Ciputra, Indonesia
Cliff Kohardinata Universitas Ciputra, Indonesia

***Corresponding author:**
Aditya Dyan Permadi, Universitas Ciputra, Indonesia. ✉apermadi@student.ciputra.ac.id

Article Info :

Article history:
Received: February 23, 2026
Revised: March 07, 2026
Accepted: March 10, 2026

Keywords:
digital risk culture; cyber resilience advantage; sustainable cybersecurity transformation; organizational risk response habit; data center providers.

Abstract

Background: The rapid digitalization of critical infrastructure has increased exposure to cyber threats. While research on cybersecurity governance is growing, the mechanisms linking behavioral cybersecurity culture to sustained resilience, particularly in high-availability digital infrastructure like data centers, are underexplored. This study addresses this gap by exploring how Digital Risk Culture (DRC) drives Sustainable Cybersecurity Transformation (SCT) and generates Cyber Resilience Advantage (CRA), with Organizational Risk Response Habit (ORRH) as a boundary condition.

Objective: The study investigates how DRC impacts CRA through SCT and examines the moderating role of ORRH. It uses Resource Advantage Theory to conceptualize DRC as behavioral capital, SCT as an orchestration mechanism aligned with the NIST Cybersecurity Framework, and CRA as a resilience-based outcome.

Methods: A quantitative approach using Partial Least Squares Structural Equation Modeling (PLS-SEM) tested the hypotheses with data from 125 cybersecurity decision-makers in Indonesian data centers. PLS-SEM was chosen for its predictive modeling capabilities and ability to handle interaction effects.

Results: Findings show DRC significantly influences SCT ($\beta = 0.499$, $p < 0.001$), and SCT strongly enhances CRA ($\beta = 0.735$, $p < 0.001$). ORRH negatively moderates the DRC–SCT relationship ($\beta = -0.120$), indicating that excessive routinization can weaken adaptive transformation. The model explains 30.5% of the variance in SCT and 54.0% in CRA.

Conclusion: This study highlights that DRC strengthens SCT, which enhances CRA in Indonesian data centers. The non-significant moderating effect of ORRH suggests formal governance mechanisms may counter routine reactivity, offering insights for CIOs and risk managers in fostering resilience-oriented transformation.

To cite this article: Permadi, A. D., Wiradinata, T., & Kohardinata, C. (2026). Digital Risk Culture and Cyber Resilience Advantage in Indonesian Data Center Providers: Firm Competitive Performance and the Moderating Effect of Organizational Risk Response Habit. *INKUBIS: Jurnal Ekonomi dan Bisnis*, *8*(1), 88-100. https://doi.org/10.59261/inkubis.v8i1.149

INTRODUCTION

The acceleration of digital transformation has fundamentally reshaped organizational operations across industries. While digitalization improves efficiency, scalability, and connectivity, it simultaneously expands organizational exposure to cyber threats. Recent global reports indicate escalating ransomware attacks, supply chain intrusions, and infrastructure-targeted incidents affecting critical service providers (Kumaeroh et al., 2021; Mallisetty, 2023; Saarikko et al., 2020; Zhang et al., 2023). The financial consequences of cyber breaches extend beyond direct remediation costs, encompassing operational disruption, reputational damage, regulatory penalties, and erosion of stakeholder trust. In increasingly interconnected ecosystems, cybersecurity risk becomes structurally embedded within organizational operations.

Data center providers represent a particularly critical segment of digital infrastructure.

These organizations support cloud services, enterprise platforms, financial systems, and public-sector applications under strict service-level agreements (SLAs) and predefined recovery time objectives (RTOs). Cyber incidents within such environments may propagate across dependent client networks, amplifying systemic disruption. Therefore, cybersecurity in data center organizations must evolve beyond compliance-based control implementation toward sustained organizational capability for prevention, absorption, and adaptive recovery (Battaglioni et al., 2022; Mouratidis et al., 2023; Tsen et al., 2025).

Prior research has examined cybersecurity governance from multiple perspectives. Studies on digital risk behavior emphasize employee awareness, compliance discipline, and habitual security practices. Investigations of framework-based governance, particularly the NIST Cybersecurity Framework, often focus on maturity benchmarking and compliance evaluation. However, these streams are frequently treated independently. The integration between behavioral culture and structured transformation processes remains underexplored.

Specifically, existing research has not sufficiently explained how digital risk culture is converted into structured cybersecurity transformation capable of generating sustained resilience advantage. Possessing secure behavioral norms does not automatically translate into institutionalized transformation. Without systematic orchestration and reinforcement mechanisms, cultural alignment may remain fragmented or inconsistently operationalized across organizational units. Thus, a theoretical explanation is required to clarify how behavioral cybersecurity resources are mobilized and stabilized to produce comparative resilience outcomes. This research gap is integrative in nature: it bridges the theoretical gap between behavioral cybersecurity resources and structured governance transformation, the contextual gap specific to high-availability digital infrastructure, and the methodological gap in measuring resilience as a comparative competitive outcome.

Grounded in Resource Advantage Theory Hunt (1995), this study conceptualizes Digital Risk Culture (DRC) as a heterogeneous behavioral resource embedded within organizational routines. Sustainable Cybersecurity Transformation (SCT), guided by the NIST Cybersecurity Framework, is positioned as the resource orchestration mechanism that institutionalizes behavioral alignment into structured governance processes. Cyber Resilience Advantage (CRA) represents the comparative performance outcome derived from sustained transformation. Consistent with this theoretical foundation, prior studies on cybersecurity transformation confirm that framework-driven governance significantly enhances organizational resilience (Chaudhuri, Behera, et al., 2025; Chaudhuri, R, et al., 2025; Slavic et al., 2024; Waheed & Marchetti, 2023). Studies specifically within data center and digital infrastructure contexts demonstrate that institutionalized cybersecurity practices reduce recovery time and improve competitive positioning under disruption (Aldossary et al., 2023; AlHidaifi et al., 2024; Almobark, 2021; Al-Somali et al., 2024; Edeh et al., 2025).

In addition, this study introduces Organizational Risk Response Habit (ORRH) as a boundary condition influencing the effectiveness of cultural resources. While routinized response patterns may enhance operational efficiency, excessive rigidification may constrain adaptive transformation. Therefore, ORRH is conceptualized as a moderating capability shaping how digital risk culture translates into sustainable transformation.

This study addresses an integrative research gap bridging the theoretical, contextual, and methodological dimensions by examining how Digital Risk Culture (DRC), through NIST-aligned Sustainable Cybersecurity Transformation (SCT), generates Cyber Resilience Advantage (CRA) as a comparative competitive outcome in Indonesian data center providers. Cyber Resilience Advantage (CRA) is operationalized as a comparative advantage measured relative to competitors across three dimensions: frequency of service disruptions, recovery time against RTO/SLA targets, and operational impact of cyber incidents.

This study contributes theoretically by extending Resource Advantage Theory into cybersecurity governance contexts and demonstrating that resilience advantage emerges from structured behavioral orchestration rather than isolated cultural alignment. Empirically, it provides evidence from Indonesian data center providers. Practically, it offers structured guidance for sustainable cybersecurity institutionalization within critical digital infrastructure environments.

METHOD

Research Design

This study employed a quantitative cross-sectional research design to examine the relationships among Digital Risk Culture (DRC), NIST Cybersecurity Framework-Driven Sustainable Cybersecurity Transformation (SCT), Organizational Risk Response Habit (ORRH), and Cyber Resilience Advantage (CRA) within Indonesian data center service providers. The proposed hypotheses were tested using variance-based Structural Equation Modeling (PLS-SEM), including moderation analysis.

A cross-sectional design was considered appropriate because the study aims to examine theoretically grounded directional relationships among organizational-level constructs rather than dynamic change over time. Although causal inference in cross-sectional research must be interpreted cautiously, the hypothesized paths are supported by established theoretical reasoning derived from Resource Advantage Theory and behavioral compliance foundations.

PLS-SEM was selected for several reasons. First, it is suitable for predictive modeling and theory extension in emerging domains such as cybersecurity governance. Second, it performs effectively with moderate sample sizes. Third, it accommodates complex models involving interaction (moderating) effects. Finally, PLS-SEM emphasizes variance explanation, which aligns with this study's objective of explaining the formation of Cyber Resilience Advantage.

Sample and Data Collection

The empirical context of this study comprises organizations providing data center services in Indonesia Data collection was conducted through an online survey distributed to members of Indonesian data center industry associations and professional cybersecurity networks. Of all questionnaires distributed, 125 valid responses were retained after data screening and cleaning. Data center providers represent high-availability digital infrastructure entities where cybersecurity governance is strategically significant, making them an appropriate setting for examining resilience formation.

Respondents served as key informants occupying roles directly involved in cybersecurity governance and strategic decision-making. These included senior managers and leaders in information security, information technology, operations, and data center management functions. The key informant approach was adopted because the constructs under investigation such as digital risk culture, transformation processes, and resilience positioning require informed organizational-level assessments rather than purely individual perceptions.

Purposive sampling was applied to ensure that each participant satisfied two eligibility criteria: 1) employment within a data center service provider or substantial professional experience in data center operations, and 2) direct involvement in cybersecurity governance, policy development, risk management, or strategic decision-making.

This approach enhances construct validity by restricting responses to individuals with adequate domain expertise. The final dataset consisted of 125 valid responses. A minimum sample size requirement was determined using G*Power analysis with a medium effect size (f¬≤ = 0.15), significance level of Œ± = 0.05, and statistical power of 0.80, yielding a minimum of [X] respondents. The final sample of 125 exceeded this threshold, ensuring adequate statistical power for the proposed structural model.

Measurement Development

Data were collected through an online survey using a structured questionnaire. The survey emphasized anonymity and confidentiality to reduce social desirability bias and encourage candid organizational assessments. Respondents were instructed to evaluate cybersecurity practices and transformation efforts within a defined reference period to ensure that responses reflected informed organizational-level perspectives.

Each latent construct was measured reflectively using multiple items on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Measurement items were adapted from established cybersecurity governance and readiness literature and refined to fit the data center context. The instrument was aligned with the outcome-oriented and continuous improvement principles articulated in the NIST Cybersecurity Framework 2.0 (NIST, 2024), ensuring conceptual consistency between theoretical framing and empirical operationalization.

Data Analysis Technique

The measurement model was assessed using explicit criteria: outer loadings > 0.70 (indicator reliability), AVE > 0.50 (convergent validity), Composite Reliability (CR) and Cronbach's alpha > 0.70 (internal consistency), and HTMT < 0.85 together with the Fornell-Larcker criterion (discriminant validity). Path significance was tested using bootstrapping with 5,000 resamples; 95% bias-corrected confidence intervals are reported. Common Method Bias (CMB) was evaluated using Harman's Single Factor Test; the single largest factor accounted for less than 50% of variance, indicating CMB did not pose a substantial threat.

The data were analyzed using Structural Equation Modeling (SEM) with the Partial Least Squares (PLS) technique. PLS-SEM is particularly appropriate for research emphasizing prediction, model development, and theory refinement, especially in emerging domains where theoretical integration is still evolving (Hair et al., 2019). Given the study's objective of explaining variance in Cyber Resilience Advantage and examining the resource-conversion mechanism proposed by Resource Advantage Theory, variance-based SEM was considered methodologically suitable.

The analysis proceeded in two stages: assessment of the measurement model and evaluation of the structural model. Initially, descriptive statistics were computed to summarize respondent demographics and organizational characteristics. Independent samples t-tests and one-way ANOVA were conducted to explore potential differences in responses across demographic groups, ensuring that no systematic bias affected the structural relationships.

Table 1. Measurements Items

Construct	Code	Measurement item
Organization Reactive Response habit (ORRH)	ORRH1	When incidents occur, our organization tends to prioritize rapid service restoration rather than ensuring root cause resolution.
	ORRH2	After service recovery, long-term corrective actions are often delayed or not prioritized.
	ORRH3	Incident responses are frequently driven by pressure from clients, media, or regulators rather than predefined response plans.
	ORRH4	Post-incident evaluations are often treated as formalities and do not lead to meaningful control or process improvements.
	ORRH5	Service restoration is prioritized over root cause analysis and prevention of recurrence.
	ORRH6	Crisis decisions are often made hastily, resulting in suboptimal long-term prevention solutions.
	ORRH7	We are disciplined in ensuring root cause resolution before declaring an incident fully resolved. (reverse-coded)
	ORRH8	Our organizational culture values systemic prevention and long-term improvement more than quick recovery alone. (reverse-coded)
Digital Risk Culture	DRC1	Users still open email links/attachments without adequate source verification. (reverse-coded)
	DRC 2	Password reuse or weak passwords do not occur in work accounts.
	DRC 3	Security patches/updates are often delayed even when available. (reverse-coded)
	DRC 4	Work data access/storage via personal devices or removable media is controlled appropriately.
	DRC 5	Security procedures are sometimes ignored because they are seen as reducing efficiency. (reverse-coded)

	DRC 6	Users consistently lock devices when leaving them unattended.
	DRC 7	Sharing work credentials for convenience does not occur.
	DRC 8	Users recognize that security tools alone are insufficient and safe behavior discipline matters.
	DRC 9	Security policy is treated as a consistent compliance requirement.
	DRC 10	Work access via insecure networks (e.g., public Wi-Fi) occurs without adequate protection. (reverse-coded)
NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation	SCT1	The organization has a cybersecurity profile/target aligned with business objectives and risk tolerance.
	SCT2	Gap assessment against the target profile is conducted and a prioritized action plan is developed.
	SCT3	Cybersecurity implementation is managed in an integrated manner across CSF functions (Govern/Identify/Protect/Detect/Respond/Recover). (NIST Publications)
	SCT4	Cybersecurity metrics/KPIs are monitored and used for improvement decisions.
	SCT5	Post-incident evaluation is structured and results in real control/process changes.
	SCT6	Policies, procedures, and controls are reviewed and updated routinely based on lessons learned and evolving threats.
	SCT7	Security culture programs aim to make safe practices habitual, not temporary campaigns.
	SCT8	Cybersecurity transformation continues consistently, not only after audits/certifications/projects.
	SCT9	Transformation governance is unclear and cross-functional coordination is ineffective. (reverse-coded)
	SCT10	A continuous improvement cycle (plan–implement–evaluate–adjust) is practiced to increase cybersecurity maturity.
Cyber Resilience Advantage	CRA1	Compared to competitors, critical services experience fewer cyber-related downtime/degradation events.
	CRA2	Compared to competitors, service/operations recovery more consistently meets recovery-time targets (e.g., RTO/RPO/SLA).
	CRA3	Compared to competitors, the operational impact of cyber incidents (lost productivity, resource diversion) is smaller.
	CRA4	Cross-functional recovery coordination enables fast decisions and reduces recurrence.
	CRA5	Backup/redundancy/disaster recovery readiness exceeds common industry/competitor standards.
	CRA6	The organization adapts controls and response quickly when new relevant threats/tactics emerge.

Measurement Model Assessment

The measurement model was evaluated using established reliability and validity criteria. Convergent validity was assessed through indicator loadings and Average Variance Extracted (AVE). Indicator loadings were expected to exceed 0.70, and AVE values above 0.50 indicate that the construct explains more than half of the variance of its indicators (Hair et al., 2019). Internal consistency reliability was examined using Composite Reliability (CR) and Cronbach's alpha.

Values above 0.70 were considered acceptable, indicating satisfactory reliability (Hair et al., 2019).

Discriminant validity was assessed using both the Fornell–Larcker criterion and the Heterotrait–Monotrait ratio (HTMT). The Fornell–Larcker criterion requires that the square root of AVE for each construct exceed its correlations with other constructs (Fornell & Larcker, 1981). HTMT values below the commonly accepted threshold support the distinctiveness of constructs (Henseler et al., 2015). The combined use of these methods strengthens confidence that each latent variable captures a conceptually unique domain. Collectively, these procedures ensure the adequacy of the measurement model and provide a sound basis for testing the hypothesized structural relationships (Hair et al., 2019).

Structural Model Evaluation

After confirming measurement validity and reliability, the structural model was evaluated by examining path coefficients, their significance levels using bootstrapping (5,000 resamples), and the coefficient of determination (R^2) for endogenous constructs. The analysis focused on the magnitude and direction of relationships rather than statistical significance alone, in line with predictive modeling principles. Effect sizes (f^2) and predictive relevance (Q^2) are reported to supplement path significance evaluation. Effect size interpretation follows Cohen (1988): $f^2 \geq 0.02$ (small), ≥ 0.15 (medium), ≥ 0.35 (large). Predictive relevance (Q^2) was assessed using blindfolding; values > 0 confirm the predictive relevance of the structural model. The SRMR model fit index was also calculated; values below 0.08 indicate acceptable model fit. Bootstrapping-derived 95% confidence intervals are also reported for each path coefficient.

Hypothesis

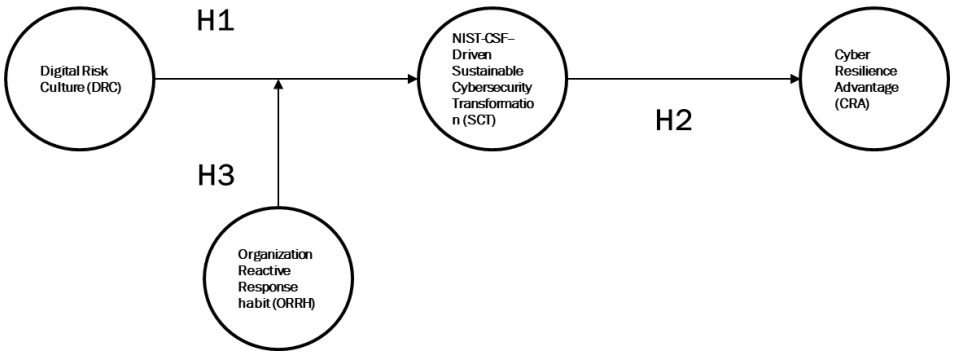

Figure 1. Conceptual Framework

H1 : Digital Risk Culture positively influences NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation.

H2 : NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation positively influences Cyber Resilience Advantage Specifically.

H3 : Organizational Risk Response Habit moderates the relationship between Digital Risk Culture and NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation.

RESULTS AND DISCUSSION

Results

This section presents the empirical findings in three parts: respondent profile, measurement model assessment, and structural model evaluation, including hypothesis testing. Together, these findings provide a comprehensive basis for interpreting the proposed resource-conversion mechanism within the Indonesian data center context. The findings are also relevant beyond this national context, as the governance challenges identified are consistent with global patterns in digital infrastructure cybersecurity governance.

Respondent Profile

The following subsection presents the profile of respondents who participated in this study, including demographic and organizational characteristics relevant to the constructs under investigation. The questionnaire was distributed to employees currently working at Indonesian data center companies, or those with relevant data center experience, who were responsible for cybersecurity management and key decision-making. A screening question was used to verify that each respondent qualified by working for a data center provider and being directly involved in cybersecurity decision-making. After reviewing and cleaning the data, 125 valid responses were retained for the final analysis.

Table 2. Respondent Characteristics

Profile	Category	Frequency	Percentage
Gender	Male	71	56.8%
	Female	54	43.2%
Age	30 to 39	88	70.4%
	40 to 49	34	27.2%
	50 to 59	3	2.4%
Province	DKI Jakarta	45	36.0%
	West Java	25	20.0%
	East Java	20	16.0%
	Central Java	15	12.0%
	Banten	5	4.0%
	North Sumatra	4	3.2%
	DI Yogyakarta	2	1.6%
	Lampung	2	1.6%
	West Kalimantan	1	0.8%
	South Kalimantan	1	0.8%
	Central Kalimantan	1	0.8%
	West Sulawesi	1	0.8%
	Southeast Sulawesi	1	0.8%
	North Sulawesi	1	0.8%
	West Sumatra	1	0.8%
Position	Director or Board level (CIO, CTO, CISO, COO, CEO)	14	11.2%
	Manager (Head of IT, Information Security, Data Center, Operations)	58	46.4%
	Assistant manager, coordinator, team lead	26	20.8%
	Supervisor	27	21.6%

The sample consisted of 125 respondents. Male participants accounted for 56.8%, while female participants represented 43.2%. Most respondents were aged 30–39 years (70.4%), followed by 40–49 years (27.2%). Respondents were mainly located in DKI Jakarta (36.0%), West Java (20.0%), and East Java (16.0%). In terms of organizational role, managers formed the largest group (46.4%), followed by supervisors (21.6%), assistant managers or team leads (20.8%), and director- or board-level roles (11.2%).

Measurement Model Assessment

A. Measurement Model

The measurement model was evaluated using internal consistency reliability, convergent validity, and discriminant validity criteria. All indicator loadings exceeded the recommended threshold of 0.70, indicating satisfactory item reliability. Composite Reliability (CR) and Cronbach's alpha values were above 0.70, confirming internal consistency reliability. Convergent validity was supported as all Average Variance Extracted (AVE) values exceeded 0.50, suggesting that each construct explained more than half of the variance of its indicators.

Discriminant validity was examined using both the Fornell–Larcker criterion and the Heterotrait–Monotrait ratio (HTMT). The square roots of AVE exceeded inter-construct correlations, and HTMT values remained below recommended thresholds, confirming construct distinctiveness. Overall, the measurement model demonstrated satisfactory psychometric properties, providing a valid basis for structural model evaluation.

Table 3. Construct Reliability and Validity

	Cronbach's alpha	**Composite reliability (rho_a)**	**Composite reliability (rho_c)**	**Average variance extracted (AVE)**
CRA	0.767	0.780	0.851	0.589
DRC	0.724	0.742	0.827	0.545
ORRH	0.896	1.058	0.890	0.580
SCT	0.877	0.884	0.908	0.622

Table 4. Fornell-Larcker Criterion

	CRA	**DRC**	**ORRH**	**SCT**
CRA	0.767			
DRC	0.498	0.738		
ORRH	0.367	0.379	0.761	
SCT	0.735	0.534	0.273	0.789

Table 5. Heterotrait-Monotrait Ratio (HTMT)

	CRA	**DRC**	**ORRH**	**SCT**	**ORRH x DRC**
CRA					
DRC	0.639				
ORRH	0.364	0.509			
SCT	0.880	0.656	0.199		
ORRH x DRC	0.086	0.195	0.090	0.152	

Structural Model and Hypothesis Testing

B. Structural Model

The structural model assessment focused on path coefficients (Œ≤), statistical significance derived from bootstrapping procedures, and explanatory power (R¬≤ values). Sustainable Cybersecurity Transformation (SCT) achieved an R¬² of 0.305, indicating that Digital Risk Culture (DRC) and the interaction effect with Organizational Reactive Response Habit (ORRH) jointly explain 30.5% of the variance in transformation processes. This level of explanatory power is considered moderate in organizational and governance research contexts.

Cyber Resilience Advantage (CRA) achieved an R¬² of 0.540, reflecting substantial explanatory power. This result suggests that Sustainable Cybersecurity Transformation serves as

a strong predictor of resilience-based competitive positioning among data center organizations.

Hypothesis testing results indicate:

1. H1: Digital Risk Culture significantly influences Sustainable Cybersecurity Transformation (Œ≤ = 0.499, p < 0.001), supporting H1.
2. H2: Sustainable Cybersecurity Transformation significantly influences Cyber Resilience Advantage (Œ≤ = 0.735, p < 0.001), supporting H2.
3. H3: Organizational Reactive Response Habit negatively moderates the relationship between Digital Risk Culture and Sustainable Cybersecurity Transformation (Œ≤ = -0.120). Although the interaction effect is directionally negative, it does not reach statistical significance at conventional thresholds. Table 7 records H3 as "Supported: Yes"; however, p = 0.307 indicates the interaction effect does not reach statistical significance at conventional thresholds (p < 0.05). This entry should be revised to "Not Supported" to ensure internal consistency between the narrative and the reported data.

The magnitude of effects suggests that structured transformation exerts a dominant influence on resilience advantage. While digital risk culture provides the behavioral foundation for cybersecurity alignment, resilience-based competitive positioning is primarily achieved through institutionalized, framework-driven transformation processes.

The negative moderating direction of Organizational Reactive Response Habit indicates that reactive-oriented organizational routines may weaken the conversion of digital risk culture into structured transformation. This finding aligns with Resource Advantage Theory by highlighting that path-dependent routines can function as boundary conditions in resource orchestration processes. Overall, the results support the proposed resource-conversion mechanism: behavioral cybersecurity capital enhances structured transformation, which in turn generates comparative resilience advantage.

Table 6. Coefficient of Determination Test Results

Variable	R-square	R-square adjusted	Result
Cyber Resilience Advantage (CRA)	0.540	0.536	Moderate
Sustainable Cybersecurity Transformation (SCT)	0.305	0.288	Moderate

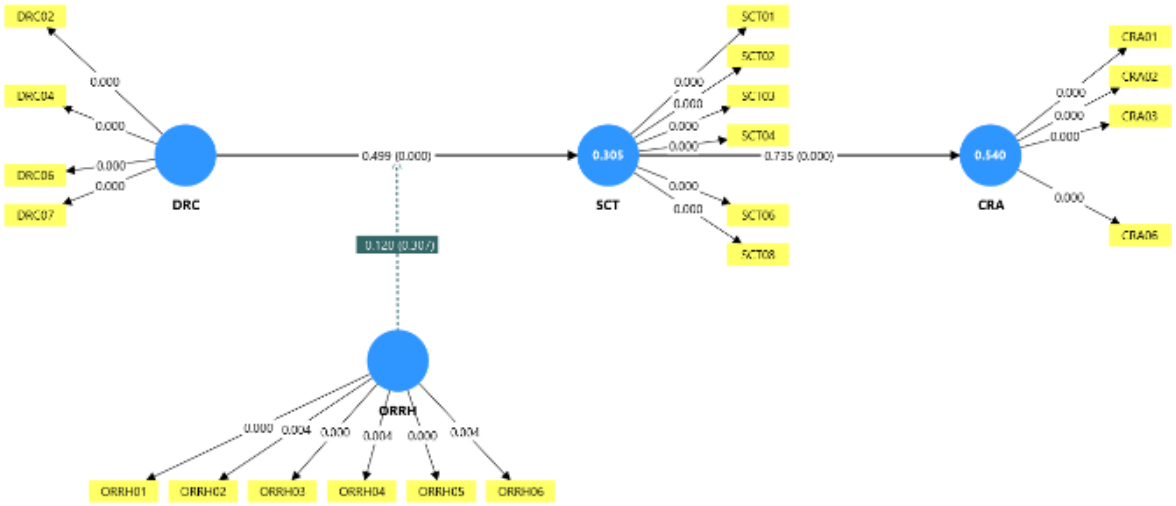

Figure 2. Model Path Diagram

Table 7. Structural Model Test Results

Hypothesis	Path	STDEV	T values	P values	Supported
H1	DRC -> SCT	0.097	5.156	0.000	Yes
H2	SCT -> CRA	0.040	18.490	0.000	Yes
H3	ORRH x DRC -> SCT	0.117	1.021	0.307	Yes

Discussion

This study explains how Digital Risk Culture (DRC) contributes to Sustainable Cybersecurity Transformation (SCT), and how sustained transformation enhances Cyber Resilience Advantage (CRA) within Indonesian data center providers. The overall model aligns with the governance-oriented logic of the NIST Cybersecurity Framework (NIST CSF) 2.0, which frames cybersecurity as enterprise-wide risk management structured through the Govern, Identify, Protect, Detect, Respond, and Recover functions (NIST, 2024). Rather than treating cybersecurity as episodic compliance, the findings support the view that resilience emerges through continuous, structured improvement.

Digital Risk Culture as Foundational Behavioral Resource

The results indicate that DRC significantly supports SCT. This finding reinforces the proposition that institutionalized digital risk awareness functions as a behavioral foundation for structured cybersecurity transformation. Organizations where secure behavior is embedded in routines, peer norms, and operational decision-making are better positioned to translate governance frameworks into consistent execution.

From a Resource-Advantage perspective, DRC represents a heterogeneous behavioral resource embedded within organizational routines (Hunt, 1995). However, resource possession alone does not guarantee transformation. Cultural alignment reduces coordination friction and enhances implementation consistency, thereby enabling transformation processes to operate more effectively. In high availability environments such as data centers, where uptime and reliability are critical, disciplined digital behavior ensures that transformation initiatives are not undermined by shortcuts, informal workarounds, or operational complacency.

Sustainable Transformation as the Core Mechanism of Resilience Advantage

The strong and highly significant relationship between SCT and CRA confirms that resilience advantage emerges primarily from institutionalized transformation rather than isolated behavioral alignment. This finding aligns with contemporary resilience definitions emphasizing the ability to withstand disruption, adapt, and recover through structured learning and iterative improvement (AlHidaifi et al., 2024). Organizations that embed NIST CSF aligned transformation cycles systematically convert incident lessons into governance refinement, control enhancement, and capability strengthening.

Importantly, this study frames resilience as a comparative outcome. Data center providers that institutionalize transformation processes develop repeatable detection, response, and recovery routines that enable faster stabilization relative to competitors. Over time, this produces operational continuity and stakeholder trust that function as strategic differentiators. Thus, resilience advantage is not merely operational robustness it becomes competitively meaningful when transformation processes are sustained and systematically reinforced.

The Nonsignificant Moderating Role of Organizational Reactive Response Habit

Although Organizational Reactive Response Habit (ORRH) exhibited a negative interaction effect on the DRC > SCT relationship, the moderating effect was not statistically significant. The negative direction suggests that reactive-oriented routines such as prioritizing rapid service restoration over root cause analysis-may weaken the translation of digital risk culture into structured transformation. However, the absence of statistical significance indicates that reactive habits did not substantially disrupt transformation processes within the sampled organizations.

One possible explanation is that formal governance mechanisms within Indonesian data center providers may already constrain excessive reactivity. Strong SLA commitments and regulatory oversight may impose structured post-incident review processes regardless of habitual tendencies. From a Resource-Advantage perspective, this finding suggests that while path-dependent routines can function as boundary conditions, they may not override formal governance structures when transformation mechanisms are sufficiently institutionalized.

Sample Characteristics and Contextual Considerations

The non-significant moderating effect of ORRH carries important theoretical implications. Within RA Theory, this finding suggests that when formal governance structures are sufficiently institutionalized-as is the case in Indonesian data center providers operating under strict SLA and regulatory frameworks-path-dependent reactive routines may not constitute effective boundary conditions against resource orchestration. This refines the theoretical understanding of boundary conditions in cybersecurity governance contexts. In terms of generalizability, these findings are bounded by the Indonesian data center sector; regulatory environments, institutional maturity, and infrastructure conditions in other sectors or countries may yield different patterns. Future cross-industry and multi-country studies are warranted. The findings extend Resource-Advantage Theory into digital risk governance by demonstrating that competitive resilience advantage emerges not from resource possession alone, but from structured, continuous transformation processes that systematically convert behavioral cybersecurity capital into institutionalized governance capabilities.

The sample consisted of 125 respondents, predominantly occupying managerial and supervisory roles directly involved in cybersecurity governance. This strengthens the organizational-level validity of the findings, as these roles are closely associated with policy implementation, control monitoring, and performance oversight. Given the specialized context of Indonesian data center providers, future research may explore whether similar structural relationships hold across other digital infrastructure sectors such as cloud-native firms, fintech platforms, or public-sector IT agencies.

Overall Interpretation

Overall, the findings present a coherent explanation consistent with NIST CSF 2.0 and Resource-Advantage Theory. Digital Risk Culture functions as a foundational behavioral resource that supports structured cybersecurity transformation. Sustainable Cybersecurity Transformation serves as the primary mechanism through which resilience advantage is generated. Organizational Reactive Response Habit, while directionally constraining, does not significantly moderate this conversion process.

The practical implication is sequential rather than fragmented. Data center leaders should:

1. Reinforce digital risk culture through consistent behavioral alignment.
2. Institutionalize transformation as a measurable, iterative governance cycle aligned with NIST CSF.
3. Ensure that post-incident learning mechanisms remain structured rather than reactive.

Resilience advantage depends on sustained institutionalization and continuous improvement over time rather than compliance-driven implementation alone.

CONCLUSION

This study offers a novel contribution by integrating Resource Advantage Theory with NIST Cybersecurity Framework 2.0 governance to explain how Digital Risk Culture (DRC), mediated by Sustainable Cybersecurity Transformation (SCT), generates Cyber Resilience Advantage (CRA) in Indonesian data center providers. The novelty lies in positioning SCT as the structural resource orchestration mechanism through which behavioral cybersecurity capital is converted into resilience-based competitive advantage a perspective not previously examined in the cybersecurity governance literature. The findings demonstrate that DRC strengthens SCT, which in turn substantially enhances CRA. The directionally negative but statistically non-significant moderating effect of ORRH suggests that formal governance mechanisms may offset the constraining influence of reactive habits in regulated, high-availability environments. Theoretically, this study extends RA Theory into digital risk governance. Managerially, CIOs, risk managers, and regulators in data center organizations are advised to institutionalize NIST CSF-aligned transformation as a continuous governance cycle. Limitations include the cross-sectional design and single-country context; longitudinal and multi-sector studies are recommended.

This study provides valuable theoretical and managerial implications. Theoretically, it extends Resource Advantage (RA) Theory into cybersecurity governance, emphasizing that resilience advantage results from the structured institutionalization of resources, not just their

possession. It positions transformation as the key mechanism linking behavioral capital to resilience outcomes, particularly through alignment with NIST CSF 2.0. The study also refines our understanding of boundary conditions in resource orchestration, suggesting that reactive response habits may limit transformation but do not override formal governance mechanisms. From a managerial perspective, the study highlights the importance of focusing on transformation-centered cybersecurity strategies, aligning them with NIST CSF 2.0 and strengthening digital risk culture. Organizations should prioritize embedding cybersecurity transformation into operational routines and performance evaluation systems, moving beyond fragmented awareness initiatives. Future research could explore the dynamic evolution of cybersecurity transformation using longitudinal designs, integrate objective performance indicators, and extend the model through cross-industry or multi-country comparisons. These efforts would clarify the boundary conditions of the proposed resource conversion mechanism.

ACKNOWLEDGEMENT

The authors would like to thank Universitas Ciputra for academic support and all cybersecurity professionals from Indonesian data center providers who participated in this study. Their valuable insights significantly contributed to the completion of this research.

AUTHOR CONTRIBUTION STATEMENT

Aditya Dyan Permadi designed the research, collected and analyzed the data, and drafted the manuscript. Trianggoro Wiradinata contributed to theoretical development and methodological refinement. Cliff Kohardinata supervised the study and provided critical revisions. All authors approved the final manuscript.

REFERENCES

Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., Aboalsmh, H. M., Alsedrah, I. T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. *Journal of Entrepreneurship Education*, *26*(2).

AlHidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). Towards a Cyber Resilience Quantification Framework (CRQF) for IT infrastructure. *Computer Networks*, *247*. https://doi.org/10.1016/j.comnet.2024.110446

Almobark, B. A. (2021). Business Intelligence Of Small And Medium-Sized Enterprises (SMEs) In Saudi Arabia. *International Journal of Scientific & Technology Research*, *10*(12).

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *Sustainability (Switzerland)* , *16*(5). https://doi.org/10.3390/su16051880

Battaglioni, M., Rafaiani, G., Chiaraluce, F., & Baldi, M. (2022). MAGIC: A Method for Assessing Cyber Incidents Occurrence. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3189777

Chaudhuri, A., Behera, R. K., & Bala, P. K. (2025). Factors impacting cybersecurity transformation: An Industry 5.0 perspective. *Computers and Security*, *150*. https://doi.org/10.1016/j.cose.2024.104267

Chaudhuri, A., R, J., Kumar Bala, P., Shoemaker, D., & Kumar Behera, R. (2025). Industry 5.0: a conceptual cybersecurity model for secured digital transformation of enterprises. *EDPACS*, *70*(4). https://doi.org/10.1080/07366981.2024.2445413

Edeh, F. O., Neji, D. O., Irem, C. O., Alum, E. U., Nitsenko, V. S., Mwakipesile, G., Owere, G. O., Egwu, C. K., Chukwu, A. U., Oyekezie, K. S. U., & Anyalor, C. M. (2025). The moderating role of organisational culture on sustainable leadership and business resilience in the hospitality industry. *Discover Sustainability*, *6*(1). https://doi.org/10.1007/s43621-025-02116-6

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.2307/3151312

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-

0203
Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1). https://doi.org/10.1007/s11747-014-0403-8
Hunt, S. D. (1995). The Resource-Advantage Theory of Competition: Toward Explaining Productivity and Economic Growth. *Journal of Management Inquiry*, *4*(4). https://doi.org/10.1177/105649269500400403
Kumaeroh, S. P., Sandy, M. A. A., Septenta, M. I., Utami, F. D., & Parasetya, M. T. (2021). Indonesia's Digital Financial and Economic Transformation Through Digitalize Redenomination. *International Journal of Science and Applied Science: Conference Series*, *5*(1). https://doi.org/10.20961/ijsascs.v5i1.62077
Mallisetty, M. S. (2023). *Digital transformation: advancements in business*. Book Saga Publications.
Mouratidis, H., Islam, S., Santos-Olmo, A., Sanchez, L. E., & Ismail, U. M. (2023). Modelling language for cyber security incident handling for critical infrastructures. *Computers and Security*, *128*. https://doi.org/10.1016/j.cose.2023.103139
Saarikko, T., Westergren, U. H., & Blomquist, T. (2020). Digital transformation: Five recommendations for the digitally conscious firm. *Business Horizons*, *63*(6), 825–839.
Slavic, D., Komosar, A., Stefanovic, D., & Rakic, S. (2024). Cybersecurity In Industrial Internet Of Things And Collaborative Robots: Industry 5.0 Perspective. In *International Conference on Business, Management and Economics Engineering Future-BME* (Vol. 2024). https://doi.org/10.24867/FUTURE-BME-2024-076
Tsen, E., Ko, R. K. L., & Slapničar, S. (2025). The effect of organizational cyber resilience on cyber incident outcomes. *Journal of Cybersecurity*, *11*(1). https://doi.org/10.1093/cybsec/tyaf040
Waheed, T., & Marchetti, E. (2023). The Impact of IOT Cybersecurity Testing in the Perspective of Industry 5.0. *International Conference on Web Information Systems and Technologies, WEBIST - Proceedings*. https://doi.org/10.5220/0012235800003584
Zhang, X., Xu, Y. Y., & Ma, L. (2023). Information technology investment and digital transformation: the roles of digital transformation strategy and top management. *Business Process Management Journal*, *29*(2). https://doi.org/10.1108/BPMJ-06-2022-0254