MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 932-937

From Cyber Capability to Resilience Advantage: A Resource-Oriented Model of Sustainable Cybersecurity Transformation in Data Center Providers

Aditya Dyan Permadi[*1], Trianggoro Wiradinata[2], Cliff Kohardinata[3]
[1]Department of Management, School of Business and Management, Universitas Ciputra, Surabaya, Indonesia
[2]Department of Informatics, School of Information Technology, Universitas Ciputra, Surabaya, Indonesia
[3]Department of Accounting, School of Business and Management, Universitas Ciputra, Surabaya, Indonesia
Email: apermadi@student.ciputra.ac.id[1*]; twiradinata@ciputra.ac.id[2]; ckohardinata@ciputra.ac.id[3]

Abstract

The increasing sophistication of cyber threats has shifted cybersecurity from a compliance driven function to a strategic capability imperative. However, prior research remains fragmented across structural readiness, digital risk behavior, and framework based maturity perspectives, offering limited explanation of how cybersecurity resources are converted into sustained resilience advantage. Grounded in Resource Advantage Theory, this study develops an integrative model positioning Cyber Capability and Readiness (CCR) and Digital Risk Culture (DRC) as heterogeneous resource bases, Sustainable Cybersecurity Transformation (SCT) aligned with the NIST Cybersecurity Framework as a resource orchestration mechanism, and Cyber Resilience Advantage (CRA) as a comparative performance outcome. Data were collected from 125 cybersecurity decision makers in Indonesian data center providers and analyzed using Partial Least Squares Structural Equation Modeling (PLS SEM). The findings indicate that CCR exerts a strong positive influence on SCT, while DRC plays a complementary yet significant role. Furthermore, SCT significantly enhances CRA, confirming the importance of institutionalized transformation in resilience formation. The study extends Resource Advantage Theory into cybersecurity governance contexts and reframes resilience as comparative advantage rather than merely operational capability. Managerially, it provides guidance for digital infrastructure organizations seeking to institutionalize sustainable cybersecurity transformation.

Keywords: Digital Risk Behavior, Cyber Capability Readiness, Sustainable Cybersecurity Transformation, Cyber Resilience Advantage, NIST CSF, Data Center Providers.

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. 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 capable of prevention, absorption, and adaptive recovery.

Prior research has addressed cybersecurity readiness, digital risk behavior, and framework-based governance from distinct perspectives. Studies on cybersecurity readiness emphasize structural capability dimensions such as governance clarity, risk management formalization, and detection capacity. Research on digital risk behavior highlights employee compliance, awareness, and habitual security practices. Meanwhile, investigations of the NIST Cybersecurity Framework largely focus on maturity benchmarking and compliance evaluation. Although each stream contributes valuable insight, integration across these domains remains limited.

Specifically, existing research has not sufficiently explained how structural readiness and digital risk culture interact within a structured transformation process to produce sustained resilience advantage. Possessing cybersecurity resources does not automatically translate into resilience. Without systematic orchestration and behavioral stabilization, capability accumulation may remain fragmented or inconsistently applied. Thus, a theoretical explanation is needed to clarify how heterogeneous cybersecurity resources are deployed and institutionalized to generate comparative resilience advantage.

Grounded in Resource Advantage Theory (RA Theory), this study conceptualizes Cyber Capability and Readiness (CCR) and Digital Risk Culture (DRC) as heterogeneous organizational resources. Sustainable Cybersecurity Transformation (SCT), guided by the NIST Cybersecurity Framework, is positioned as the resource orchestration mechanism. Cyber Resilience Advantage (CRA) represents the comparative outcome derived from structured resource deployment. By integrating structural capability, behavioral culture, and framework-driven transformation, this study aims to provide a coherent explanation of resilience formation within data center organizations.

Accordingly, this study examines
(1) the influence of CCR on SCT,
(2) the influence of DRC on SCT, and
(3) the impact of SCT on CRA.

The study contributes theoretically by extending RA Theory into cybersecurity governance contexts, empirically by providing evidence from Indonesian data center providers, and practically by offering structured guidance for sustainable cybersecurity institutionalization.

Literature Review

Cyber Capability and Readiness

Cyber Capability and Readiness (CCR) refers to an organization's structured capacity to establish, manage, and continuously enhance cybersecurity practices through the integration of technological and non-technological elements. This construct encompasses:
(1) cybersecurity leadership and accountability structures,
(2) formalized risk management processes and standard operating procedures,
(3) technical capabilities for monitoring, detection, response, and recovery, and
(4) human capital components such as training, awareness, and disciplined security behavior.

CCR therefore reflects coordinated organizational alignment, in which governance provides direction, processes ensure consistency, technological infrastructure operationalizes controls, and human capabilities sustain compliance and adaptation.

Recent research on cybersecurity preparedness supports this multidimensional perspective. Systematic reviews indicate that readiness is not determined solely by technological investment; rather, organizational structures, managerial commitment, and human competencies significantly influence the reliability and sustainability of cybersecurity controls over time (Nillasithanukroh et al., 2025). These findings suggest that preparedness functions as an integrated organizational capability rather than as a collection of isolated technical safeguards. However, much of the existing literature conceptualizes readiness primarily as a maturity state or compliance level. This perspective underestimates its strategic role as a heterogeneous resource configuration that can enable structured cybersecurity transformation. From a Resource Advantage perspective, organizations possessing stronger cybersecurity capability and readiness are better positioned to institutionalize framework-driven transformation initiatives because they possess the structural and procedural foundations necessary for consistent implementation and continuous improvement.

Accordingly, it is proposed that:
H1: Cyber Capability and Readiness positively influences NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation.

Digital Risk Culture

Digital Risk Culture (DRC) shapes how employees perceive, interpret, and manage cybersecurity risks in their daily organizational activities. It reflects the extent to which security awareness is embedded within decision-making routines, peer expectations, informal norms, and habitual practices across the organization. Rather than being limited to formal training programs, DRC captures the institutionalization of secure behavior as a shared organizational value.

A strong digital risk culture promotes consistent compliance with security controls, cautious engagement with digital content, and responsible use of organizational systems and devices. It aligns individual behavior with formal governance structures and technical safeguards, thereby reducing implementation gaps between policy design and operational execution. In this sense, DRC functions as behavioral capital that stabilizes cybersecurity routines.

Behavioral research grounded in the Theory of Planned Behavior and the Theory of Interpersonal Behavior explains that attitudes, subjective norms, perceived behavioral control, and habitual reinforcement shape compliance behavior. Recent studies reinforce this perspective by demonstrating that cybersecurity awareness becomes more effective when treated as an organizational capability rather than a one-off intervention (Baltuttis et al., 2024). Similarly, Bishop (2025) argues that cybersecurity awareness should be conceptualized as a built-in organizational competency integrating knowledge, attitudes, and habitual discipline rather than episodic training sessions.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 932-937

However, prior research predominantly examines digital risk behavior at the individual level, with limited integration into organizational transformation frameworks. This creates a conceptual gap regarding how behavioral alignment supports structured cybersecurity institutionalization. From a Resource Advantage perspective, when digital risk culture is embedded as organizational behavioral capital, it enhances the consistency and durability of cybersecurity initiatives. It provides the human foundation necessary for framework-driven transformation processes to operate effectively and evolve over time.

Accordingly, it is proposed that:

H2: Digital Risk Culture positively influences NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation.

NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation

NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation (SCT) refers to a deliberate and continuous organizational change process that enhances cybersecurity risk management by systematically aligning governance, processes, and capabilities with the NIST Cybersecurity Framework (NIST, 2024). Rather than representing a compliance exercise or episodic remediation effort, SCT reflects institutionalized improvement cycles embedded within leadership structures, strategic decision-making, operational routines, and organizational learning mechanisms.

In this study, sustainable transformation encompasses four interrelated dimensions:

(1) alignment of leadership roles and accountability structures;

(2) systematic refinement of processes and security controls consistent with the NIST CSF functions (Govern, Identify, Protect, Detect, Respond, Recover);

(3) development of employee competencies and disciplined security routines that normalize secure behavior; and

(4) iterative learning derived from performance reviews, audits, and incident analyses.

This multidimensional view aligns with contemporary transformation research emphasizing that cybersecurity evolution is shaped not only by technological upgrades but also by leadership quality, process maturation, training reinforcement, and institutional discipline (Chaudhuri et al., 2025). However, prior studies predominantly conceptualize transformation as implementation progress or maturity benchmarking. Limited research positions transformation explicitly as a mediating organizational mechanism that converts heterogeneous cybersecurity resources into resilience-based advantage.

From a Resource Advantage Theory perspective, SCT functions as the resource orchestration mechanism through which structural readiness (CCR) and behavioral capital (DRC) are systematically deployed and institutionalized. Without structured transformation, readiness resources may remain fragmented and behavioral alignment may lack strategic direction. When sustained over time, framework-driven transformation strengthens prevention, detection, response, and recovery capabilities in a coordinated manner. This institutionalization process enhances organizational stability during cyber disruptions and accelerates recovery cycles relative to competitors.

Accordingly, it is proposed that:

H3: NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation positively influences Cyber Resilience Advantage.

Cyber Resilience Advantage

Cyber Resilience Advantage (CRA) refers to an organization's comparative capability to maintain operational continuity, minimize service disruption, and recover more rapidly than competitors when facing cyber incidents. The emphasis on "advantage" distinguishes this construct from conventional resilience metrics. Rather than measuring internal robustness alone, CRA captures relative performance positioning under conditions of cyber disruption.

In strategic terms, resilience becomes meaningful when it allows organizations to sustain reliability, protect stakeholder trust, and preserve value creation while competitors experience prolonged disruption. A more resilient organization not only absorbs shocks but also adapts and restores operations in ways that reduce reputational damage, contractual penalties, and customer attrition. Thus, resilience constitutes a competitive differentiator in digitally intensive environments.

Recent organizational studies support this strategic perspective. Empirical evidence indicates that deeply embedded and consistently enforced cybersecurity practices enhance organizational resilience capacity and operational stability (Al-Somali et al., 2024; Tang, 2025). However, much of the existing literature treats resilience as an operational outcome of cybersecurity maturity, without explicitly framing it as a source of competitive advantage. This limits theoretical integration with broader strategic management discourse.

From a Resource Advantage Theory perspective, CRA emerges when heterogeneous cybersecurity resources are systematically orchestrated and institutionalized through sustained transformation. Readiness resources provide structural foundations, digital risk culture stabilizes behavioral alignment, and framework-guided transformation ensures coordinated deployment. When these elements operate cohesively over time, organizations develop prevention, detection, response, and recovery capabilities that are difficult to imitate. This cumulative institutionalization process produces resilience that is not merely functional but strategically advantageous.

Accordingly, within this model, Cyber Resilience Advantage is conceptualized as the outcome of ongoing, NIST CSF–driven Sustainable Cybersecurity Transformation that effectively deploys readiness resources while minimizing risky behaviors across the organization.

Theoritical Review

Resource Advantage Theory (RA Theory) Resource Advantage Theory (RA Theory) conceptualizes competition as a dynamic and continuous process in which firms achieve superior performance through the effective configuration and deployment of heterogeneous resources (Hunt, 1995; Hunt, 2012). Unlike static resource-based perspectives that emphasize mere resource possession, RA Theory underscores the importance of resource heterogeneity, imperfect mobility, and strategic orchestration in generating comparative advantage. Firms do not gain advantage simply by owning valuable resources, rather, they must organize, integrate, and deploy these resources into coherent systems that create value and enhance market performance. Within this theoretical framework, value creation emerges from structured resource alignment and capability institutionalization. Competitive advantage is therefore the outcome of resource conversion processes that transform internal strengths into market-relevant capabilities.

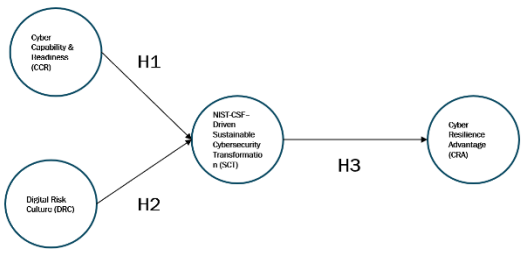
When applied to cybersecurity governance, RA Theory implies that cybersecurity-related assets such as governance structures, risk management routines, technical detection and response systems, and human competencies constitute heterogeneous organizational resources. However, these resources do not automatically produce resilience. Without systematic orchestration and institutionalization, cybersecurity practices may remain fragmented, compliance-driven, or inconsistently enforced. Sustainable resilience requires that these resources be embedded into ongoing organizational processes rather than treated as static policy instruments.

In this study, RA Theory is operationalized through a three-layer structure. First, Cyber Capability and Readiness (CCR) represents the foundational resource base, encompassing structural and procedural cybersecurity capital. Second, NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation (SCT) functions as the resource orchestration mechanism that converts readiness resources into institutionalized practices. Third, Cyber Resilience Advantage (CRA) represents the comparative performance outcome, reflecting superior continuity and recovery capability relative to competitors (Hunt, 2012).

Thus, the model advances RA Theory within cybersecurity contexts by explaining how structured transformation processes mediate the relationship between heterogeneous cybersecurity resources and resilience-based competitive advantage.

Figure 1. Conceptual Framework

Methods



Research Design

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 932-937

This study employed a quantitative cross-sectional research design to examine the relationships among Cyber Capability and Readiness (CCR), Digital Risk Culture (DRC), NIST Cybersecurity Framework–Driven Sustainable Cybersecurity Transformation (SCT), and Cyber Resilience Advantage (CRA) within Indonesian data center service providers. The proposed causal relationships (H1–H3) were tested using variance-based Structural Equation Modeling (PLS-SEM).

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 foundations.

PLS-SEM was selected due to its suitability for predictive modeling, theory development in emerging contexts, and analysis of complex models with relatively moderate sample sizes. In addition, PLS-SEM emphasizes variance explanation, which aligns with the 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 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 organizational readiness and transformation require informed, organization-level assessments rather than individual perceptions alone.

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-related governance or strategic decisions.

This approach enhances data relevance and construct validity by restricting responses to individuals with adequate domain knowledge. The final dataset consisted of 125 valid responses.

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 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
Cyber Capability and Readiness	CCR1	Roles, responsibilities, and accountability for cybersecurity are clearly defined and implemented.
	CCR2	Cyber risk and control priorities follow a formal process involving relevant business units.
	CCR3	Asset inventory and critical system mapping are maintained for risk management purposes.
	CCR4	Cybersecurity risk assessment is conducted periodically and used in decision-making.
	CCR5	Policies and procedures are documented and communicated across relevant functions.
	CCR6	Preventive controls are implemented consistently to protect critical services.
	CCR7	Monitoring and detection capabilities are in place to identify cyber threats promptly.
	CCR8	Incident response procedures are documented, roles are clear, and drills/testing have been conducted.
	CCR9	Backup, redundancy, and/or disaster recovery are managed and tested periodically.
	CCR10	Internal audits/assessments monitor compliance and control effectiveness.
	CCR11	Routine cybersecurity training and awareness programs are delivered to employees/critical roles.
	CCR12	Adequate resources (time, staff, budget) support continuous cybersecurity improvement.
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; Nunnally & Bernstein, 1994).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 932-937

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.

Results and Discussion

Respondent Profile

The survey questionnaire was sent to employees working in Indonesian data center companies or those with experience related to data centers, who handle cybersecurity management and make key decisions. A filtering question checked that each person qualified by working for a data center provider and being directly involved in cybersecurity choices. After reviewing and cleaning the data, 125 valid responses were kept for the final study.

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 organisational 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

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)
CCR	0.790	0.804	0.864	0.614
CRA	0.702	0.721	0.833	0.625
DRC	0.724	0.742	0.827	0.545
SCT	0.803	0.817	0.872	0.632

Table 4. Fornell-Larcker Criterion

	CCR	CRA	DRC	SCT
CCR	0.784			
CRA	0.645	0.790		
DRC	0.561	0.462	0.738	
SCT	0.702	0.674	0.540	0.795

Table 5. Heterotrait-Monotrait Ratio (HTMT)

	CCR	CRA	DRC	SCT
CCR				
CRA	0.861			
DRC	0.725	0.620		
SCT	0.869	0.879	0.693	

Structural Model and Hypothesis Testing

Structural Model

The structural model assessment focused on path coefficients, statistical significance, and explanatory power (R^2).

Sustainable Cybersecurity Transformation (SCT) achieved an R^2 of 0.524, indicating that Cyber Capability and Readiness (CCR) and Digital Risk Culture (DRC) jointly explain a substantial proportion of variance in transformation processes. Cyber Resilience Advantage (CRA) achieved an R^2 of 0.455, reflecting moderate explanatory power.

Hypothesis testing results indicate:

CCR significantly influences SCT (β significant, $p < 0.001$), supporting H1.

DRC significantly influences SCT (β significant, $p < 0.05$), supporting H2.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 932-937

SCT significantly influences CRA (β significant, $p < 0.001$), supporting H3.
The magnitude of effects suggests that structural readiness exerts a stronger influence on transformation compared to digital risk culture. This finding provides important insight into the layered nature of cybersecurity capability development.

Table 6. Coefficient of Determination Test Results

Variable	R-square	R-square adjusted	Result
Cyber Resilience Advantage (CRA)	0.455	0.450	Moderate
Sustainable Cybersecurity Transformation (SCT)	0.524	0.516	Moderate

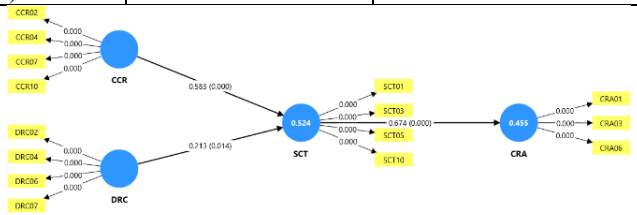


Figure 2 Model Path Diagram

Table 7. Structural Model Test Results

Hypo-thesis	Path	STDEV	T values	P values	Supported
H1	CCR > SCT	0.084	6.898	0.000	Yes
H2	DRC > SCT	0.086	2.463	0.014	Yes
H3	SCT > CRA	0.051	13.348	0.000	Yes

Discussion. This study explains how Cyber Capability and Readiness (CCR) and Digital Risk Culture (DRC) contribute 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 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.

Cyber Capability and Readiness as Foundational Resource. The results indicate that CCR significantly supports SCT. This finding reinforces the proposition that structural readiness functions as the primary enabling condition for institutionalized cybersecurity transformation. In line with the governance emphasis of NIST CSF 2.0, organizations with clearer ownership structures, asset mapping, risk prioritization routines, monitoring capabilities, and tested recovery procedures are better positioned to operationalize continuous improvement cycles (NIST, 2024).From a Resource-Advantage perspective, CCR represents the heterogeneous organizational resource base (Hunt, 1996; Hunt & Morgan, 1995). Transformation does not occur automatically from resource possession; however, when readiness is sufficiently developed, it lowers coordination friction and enhances repeatability of improvement processes. In high-availability environments such as data centers,where reliability targets and strict change controls are mandatory, structural preparedness becomes a precondition for sustained transformation rather than a peripheral support mechanism.

Digital Risk Culture as Behavioral Stabilizer. The findings also show that DRC positively influences SCT. This relationship can be explained through behavioral theory. According to the Theory of Planned Behavior (Ajzen, 1991), behavior is shaped by attitudes, subjective norms, and perceived behavioral control. In cybersecurity settings, compliance behavior depends not only on awareness but also on whether secure actions are perceived as feasible within operational contexts (Ifinedo, 2012).

Moreover, the Theory of Interpersonal Behavior (Triandis, 1977) highlights the role of habits and facilitating conditions. This helps clarify why Digital Risk Culture contributes to transformation sustainability. When secure routines are reinforced through daily practice and supported by enabling environments, transformation programs are less vulnerable to shortcuts and informal workarounds. Consistent with evidence reviews (Sommestad et al., 2019), behavioral theories alone do not fully explain cybersecurity outcomes. Organizational conditions remain critical. Thus, the results suggest a layered capability structure: CCR provides structural grounding, while DRC stabilizes execution.

Sustainable Transformation as Mechanism for Resilience Advantage. The strong relationship between SCT and CRA confirms that resilience advantage emerges from institutionalized transformation rather than isolated investments. This finding aligns with contemporary resilience definitions emphasizing the ability to withstand disruption, adapt, and recover through continuous learning (AlHidaifi et al., 2024; World Economic Forum, 2024).

Importantly, this study frames resilience as comparative advantage. Organizations that embed continuous improvement cycles aligned with NIST CSF functions develop repeatable detection, response, and recovery routines. Incident lessons are systematically translated into process updates and control enhancements. Over time, this creates operational stability and faster recovery relative to competitors. This perspective extends resilience literature by integrating governance frameworks and competitive positioning logic. Resilience is not merely operational robustness it becomes a strategic differentiator when institutionalized.

Sample Characteristics and Contextual Considerations. The demographic profile strengthens the organizational relevance of the findings. The sample consisted of 125 respondents, predominantly aged 30–39 and occupying managerial or supervisory roles. These positions are closely associated with governance oversight, control implementation, and performance monitoring, which are central to CCR and SCT.However, prior evidence suggests that cybersecurity behavior may vary across age groups and organizational contexts (Hadlington, 2018). Future studies may therefore apply multi-group analysis to examine whether structural and behavioral effects differ across hierarchical or demographic segments.

Overall Interpretation. Overall, the findings present a coherent explanation consistent with NIST CSF 2.0 and Resource-Advantage Theory. Cyber Capability and Readiness and Digital Risk Culture jointly support Sustainable Cybersecurity Transformation, and sustained transformation builds Cyber Resilience Advantage.

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

1. Strengthen structural readiness foundations.
2. Reinforce digital risk culture through facilitating conditions.
3. Institutionalize transformation as a measurable, iterative governance cycle.

Resilience advantage depends on sustained learning and improvement over time rather than compliance-driven implementation (World Economic Forum, 2024).

Conclusions and Implications

Conclusions

This study examined the structural relationships among Cyber Capability and Readiness (CCR), Digital Risk Culture (DRC), Sustainable Cybersecurity Transformation (SCT), and Cyber Resilience Advantage (CRA) within Indonesian data center service providers, using the NIST Cybersecurity Framework (CSF) 2.0 as a guiding reference.

The empirical findings demonstrate three key results. First, Cyber Capability and Readiness significantly strengthen Sustainable Cybersecurity Transformation. Second, Digital Risk Culture also contributes positively to Sustainable Cybersecurity Transformation, although with a comparatively smaller effect size. Third, Sustainable Cybersecurity Transformation significantly enhances Cyber Resilience Advantage.The relative strength of CCR compared to DRC indicates that structural readiness such as governance clarity, formalized risk management processes, monitoring capabilities, incident response preparedness, and resource allocation plays a primary enabling role in sustaining cybersecurity transformation. Cultural alignment, while important, functions as a reinforcing mechanism rather than the core structural driver.Overall, the results suggest that cyber resilience advantage does not emerge directly from isolated security controls or episodic initiatives. Instead, it is developed through institutionalized, framework aligned transformation processes that systematically convert organizational capability into repeatable operational routines across the Govern–Recover cycle of NIST CSF 2.0.

Theoretical Implications

This study contributes to Resource Advantage (RA) Theory by extending its application into the cybersecurity governance domain. Consistent with RA Theory, heterogeneous organizational resources require structured deployment to produce competitive outcomes. In this model:

a. CCR represents the strategic resource base,
b. SCT functions as the resource conversion mechanism,
c. CRA represents the realized competitive position.

The findings empirically support the argument that resilience advantage is not resource possession per se, but the outcome of resource configuration and routinization.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 932-937

Second, the study contributes to cybersecurity governance literature by integrating structural readiness and behavioral culture within a framework driven transformation process. Prior research often isolates structural maturity or behavioral compliance. This study demonstrates that transformation mediates the pathway through which readiness and culture translate into measurable resilience outcomes.Third, the study advances digital infrastructure research by contextualizing cyber resilience within high availability environments such as data centers, where uptime, operational continuity, and recovery performance are mission critical.

Managerial Implications. From a managerial perspective, the results suggest that data center providers should prioritize capability-first transformation strategies.

Given the stronger influence of CCR on SCT, organizations are encouraged to:

a. Strengthen executive-level cybersecurity governance,
b. Formalize risk-based prioritization mechanisms,
c. Enhance detection and response maturity,
d. Institutionalize recovery testing and performance measurement,
e. Allocate sufficient cybersecurity budgets and skilled personnel.

Digital Risk Culture should be reinforced systematically through:

a. Clear behavioral expectations,
b. Reduction of friction in compliance processes,
c. Integration of secure behavior into performance metrics,
d. Continuous awareness programs embedded into operational routines.

Rather than treating culture and capability as parallel initiatives, organizations should design transformation programs where behavioral reinforcement supports structurally defined controls.Sustainable Cybersecurity Transformation should be institutionalized through measurable target profiles, periodic gap assessments, structured incident learning cycles, and continuous maturity development aligned with NIST CSF 2.0.

Limitations and Future Research. Despite its contributions, this study has several limitations that should be acknowledged.

First, the use of a cross-sectional design restricts the ability to observe the dynamic evolution of cybersecurity transformation and resilience advantage over time. Although the proposed relationships are theoretically grounded, the accumulation and institutionalization of cybersecurity capabilities are inherently longitudinal processes. Future research should adopt longitudinal or panel designs to examine how capability development, cultural reinforcement, and resilience performance co-evolve across multiple time periods.

Second, the study relies on perceptual assessments provided by key informants. While respondents were selected based on their involvement in cybersecurity governance and strategic decision-making, subjective evaluations may not fully capture operational performance outcomes. Subsequent research may integrate objective indicators such as incident frequency, mean time to detect (MTTD), mean time to respond (MTTR), recovery duration, service downtime metrics, and audit findings to strengthen measurement robustness and triangulate findings.Third, the empirical context is confined to Indonesian data center service providers. Although this setting offers high relevance due to its operational criticality and regulatory exposure, institutional, regulatory, and technological conditions may vary across industries and countries. Therefore, caution should be exercised in generalizing the findings beyond similar high-availability digital infrastructure environments.Future studies may extend the model through cross-industry comparisons, multi-country investigations, or multi-group analyses examining whether structural readiness and digital risk culture exert different effects across organizational maturity levels, regulatory regimes, or hierarchical positions. Such extensions would further clarify the boundary conditions of the proposed resource-conversion mechanism.

References

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Al Janabi, S., Nunes, P., & Bresciani, S. (2024). Ongoing cybersecurity evolution: Risk and compliance in continuous improvement cycles. Information, 15(7), 420. https://doi.org/10.3390/info15070420

AlHidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). Towards a Cyber Resilience Quantification Framework (CRQF) for IT infrastructure. Computer Networks, Article 110446. https://doi.org/10.1016/j.comnet.2024.110446

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, 16(5), 1880. https://doi.org/10.3390/su16051880

Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. Computers & Security, 140, 103741. https://doi.org/10.1016/j.cose.2024.103741

Bishop, L. M. (2025). The employee cybersecurity awareness framework. Human Behavior and Emerging Technologies, 2025, 1025045. https://doi.org/10.1155/hbe2/1025045

Chaudhuri, K., Ghosh, A., Kumar, A., & Bose, I. (2025). Factors impacting cybersecurity transformation: An Industry 5.0 perspective. Computers & Security, 149, 104267. https://doi.org/10.1016/j.cose.2024.104267

ENISA. (2024). ENISA Threat Landscape 2024 (September 2024). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 PDF: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.pdf

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

Hadlington, L. (2018). Employees' attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. International Journal of Cyber Criminology, 12(1). https://www.cybercrimejournal.com/pdf/HadlingtonVol12Issue1IJCC2018.pdf

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, 115–135. 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), 317–332. https://doi.org/10.1177/105649269500400403

Hunt, S. D. (2010). Marketing theory: Foundations, controversy, strategy, and resource-advantage theory. Routledge.

Hunt, S. D., & Morgan, R. M. (1995). The comparative advantage theory of competition. Journal of Marketing, 59(2), 1–15. https://doi.org/10.1177/002224299505900201

Hunt, S. D., & Morgan, R. M. (1996). The resource-advantage theory of competition: Dynamics, path dependencies, and evolutionary dimensions. Journal of Marketing, 60(4), 107–114. https://doi.org/10.1177/002224299606000410

IBM Security, & Ponemon Institute. (2024). Cost of a data breach report 2024. https://www.ibm.com/reports/data-breach PDF: https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Nillasithanukroh, S., Seethamraju, R., & Walker, R. (2025). Enhancing preparedness: A systematic review of cybersecurity preparedness and practical implementation. Technology in Society, 83, 103042. https://doi.org/10.1016/j.techsoc.2025.103042

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (CSWP 29). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.

Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. Journal of Computer Information Systems. PDF: https://sommestad.com/teodor/papers/Sommestad%2C%20Karlz%C3%A9n%2C%20Hallberg%20-%202019%20-%20The%20Theory%20of%20Planned%20Behavior%20and%20Information%20Security%20Policy%20Compliance.pdf

Tang, R., & Li, M. (2025). Cybersecurity and corporate resilience: A study based on listed companies in China. Structural Change and Economic Dynamics. ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0160791X25002957

Triandis, H. C. (1977). Interpersonal behavior. Brooks/Cole.

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/