International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Business Analytics Capability and Organizational Cyber Resilience: The Roles of Data-Driven Risk Detection and Cybersecurity Governance

Vo Minh Vinh[1], Mai Le Ba Thanh[2], Le Phuong Chi[3]
[1] Faculty of Management and Economics, Tomas Bata University, Czech Republic
Orcid: https://orcid.org/0009-0007-4100-770X
[2] Vietnam Australia International School, Ho Chi Minh, Vietnam
[3] Hung Vuong High School for gifted students, Phu Tho Province, Vietnam

ABSTRACT: This study examines the relationships among business analytics capability, data driven risk detection, and organizational cyber resilience while evaluating the moderating influence of cybersecurity governance maturity. Drawing on Dynamic Capabilities Theory and Organizational Information Processing Theory, it conceptualizes organizational cyber resilience as the outcome of organizational capabilities that transform integrated analytical resources and cyber risk information into timely, coordinated, and adaptive responses. Cybersecurity governance maturity serves as a boundary condition that determines whether analytical insights can be translated into stronger resilience outcomes. A quantitative cross-sectional design gathered responses through a five point Likert scale questionnaire from 385 Vietnamese professionals knowledgeable about business analytics, cybersecurity, information technology, risk management, digital operations, organizational governance, or business continuity. IBM SPSS version 26 supported reliability assessment, exploratory factor analysis, and multiple linear regression, while Hayes' Process Macro Model 1 examined the moderating effect. The findings show that business analytics capability ($\beta = 0.573$) and data driven risk detection ($\beta = 0.638$) significantly improve organizational cyber resilience. Data driven risk detection produces the stronger direct effect, emphasizing the importance of continuous monitoring, anomaly identification, and actionable cyber risk warnings. Cybersecurity governance maturity further strengthens the positive relationship between business analytics capability and organizational cyber resilience through a significant interaction coefficient of 0.407. The results demonstrate that analytical technologies alone cannot guarantee cyber resilience. Organizations must combine integrated analytical resources and timely risk detection with clear accountability, formal escalation procedures, structured oversight, continuous governance improvement, and sufficient authority to coordinate responses.

KEYWORDS: organizational cyber resilience; business analytics capability; data-driven risk detection; cybersecurity governance maturity; cybersecurity analytics.

1. INTRODUCTION

Organizational cyber resilience represents a pressing research challenge, as digitally reliant firms must go beyond merely blocking attacks to also foresee, endure, react to, and rebound from disruptions while preserving essential functions. With threats growing ever more advanced and inevitable, traditional defense-focused cybersecurity falls short; true resilience demands ongoing adaptation, organizational learning, and synchronized recovery (Dupont et al., 2023). Yet current evaluation frameworks stay disjointed, poorly defined, and weakly tested across sectors, leaving organizations hard-pressed to gauge real readiness (Sepúlveda Estay et al., 2020). Cyber resilience further needs framing as a dynamic organizational capability instead of a fixed set of technical measures, since success hinges on how companies reallocate resources and draw lessons from incidents (Goel et al., 2023). Studies also show that resilience efforts require tailoring to each firm's setting, though many still deploy off-the-shelf tools without weaving in managerial judgment or governance structures (Annarelli et al., 2020). Thus, investigating whether business analytics capability and data-driven risk detection bolster cyber resilience, and whether cybersecurity governance maturity amplifies that effect, remains essential for clarifying how organizations turn mounting security data into prompt detection, coordinated action, and lasting operational continuity.

Earlier work frames cyber resilience as an organization's ability to anticipate, endure, recover from, and adapt after cyber disruption. Most studies, however, have concentrated on building assessment tools or managerial guidelines instead of clarifying the

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

organizational factors that produce it (Annarelli et al., 2020; Sepúlveda Estay et al., 2020). Goel et al. (2023) moved the discussion forward by viewing information-security resilience as a dynamic capability, and Dupont et al. (2023) highlighted the gap between resilience rhetoric and actual practice. Empirical findings stay mixed: Tsen et al. (2025) observed stronger resilience among firms that had not been attacked, yet higher resilience did not clearly lessen the fallout of incidents. Such inconsistencies likely stem from limited samples, reliance on self-reported cross-sectional data, confidentiality bias, and the habit of treating resilience as a fixed state. More importantly, existing research stresses technical safeguards, broad preparedness, or incident results, while largely overlooking how analytical resources actually create resilience. As a result, few empirical studies bring business analytics capability, data-driven risk detection, and cybersecurity governance together in a single explanatory model. This study fills this gap by testing the direct effects of business analytics capability and data-driven risk detection on organizational cyber resilience and by checking whether cybersecurity governance maturity intensifies the analytics–resilience link. The resulting model shows when analytics functions as a genuine operational resilience capability rather than simply a technological asset.

This study addresses three research questions: (1) To what extent does business analytics capability shape organizational cyber resilience? (2) How does data-driven risk detection influence organizational cyber resilience? (3) How does cybersecurity governance maturity moderate the link between business analytics capability and organizational cyber resilience? It, therefore, tests the direct effect of business analytics capability on cyber resilience, evaluates the impact of data-driven risk detection, and explores whether governance maturity intensifies the analytics–resilience connection. On the academic side, this paper unites analytical, risk-detection, governance, and dynamic-capability lenses in one framework, advancing business analytics and cybersecurity research by showing when analytical resources turn into effective resilience capabilities under varying governance conditions. Practically, it offers leaders, cybersecurity managers, and analytics professionals evidence for aligning analytical systems, real-time risk detection, and governance practices. Such guidance can inform cybersecurity spending, improve threat anticipation and response, limit operational disruption, speed recovery after attacks, and support the continuity of essential functions against increasingly advanced cyber threats.

2. LITERATURE REVIEW

2.1. Organizational Cyber Resilience

Organizational cyber resilience denotes a firm's ability to prepare for, absorb, recover from, and adapt after cyber incidents while sustaining core operations and safeguarding strategic value. In contrast to traditional cybersecurity's focus on preventing attacks, resilience accepts that full protection is unattainable and therefore embeds continuity, response, recovery, and adaptation (Tzavara & Vassiliadis, 2024). Its growing strategic weight stems from organizations' rising reliance on interconnected digital systems, where a single breach can halt operations, harm reputation, and erode stakeholder trust. Research on UK SMEs shows that resilience entails not only managing and recovering from incidents but also adjusting organizational resources to new threats (Fernandez de Arroyabe et al., 2024). Studies of critical infrastructure further reveal that resilience rests on combined technological, human, and managerial strengths rather than stand-alone security tools (Malatji et al., 2022). However, institutionalizing resilience proves challenging because managers view cyber risk through different lenses. Business leaders often stress continuity, while IT specialists prioritize technical defenses, producing fragmented choices before and after incidents (Bagheri et al., 2023). Thus cyber resilience is best understood not as a fixed condition of being "secure," but as a dynamic socio-technical capability whose success hinges on converting threat data into coordinated action, keeping operations running amid disruption, learning from events, and continually reshaping governance and analytical resources.

2.2. Critical Analysis of Theoretical Frameworks

The two most appropriate theories are Dynamic Capabilities Theory and Organizational Information Processing Theory. Together, they explain both the adaptive conversion of analytics into cyber resilience and the information–governance alignment required for that conversion.

2.2.1. Dynamic Capabilities Theory

Dynamic Capabilities Theory describes how firms deliberately integrate, build, and reconfigure internal and external resources amid rapid environmental shifts. Unlike ordinary capabilities that merely support routine efficiency, dynamic capabilities allow organizations to sense change, seize suitable responses, and transform resource bases to sustain competitiveness and continuity (Teece, 2018). This logic fits cyber resilience especially well, because cyber threats advance faster than fixed protective routines; a

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

resilient firm must continually spot unfamiliar attack patterns, mobilize responses, restore operations, and revise systems after incidents. Consequently, organizational cyber resilience emerges from repeated sensing, seizing, and transforming cycles rather than from owning cybersecurity tools alone. Within this view, business analytics capability acts as an enabling dynamic capability that combines data, infrastructure, technical skill, managerial insight, and data-driven processes; its value appears only when these elements generate actionable knowledge that alters organizational behavior. Empirical work shows that big-data analytics strengthens sensing, seizing, and transformation by helping firms detect environmental signals, choose responses, and reconfigure operations (Mikalef et al., 2021), while broader evidence links analytical capabilities to anticipation, coping, and adaptation across disruption phases (Al-Ghattas & Marjanovic, 2021). Data-driven risk detection constitutes the sensing mechanism that turns logs, behavioral traces, network activity, and threat intelligence into clear signals about vulnerabilities and impending attacks, thereby reducing uncertainty and enabling earlier containment. Such detection also feeds organizational learning by exposing flaws in prior assumptions and routines, which in turn supports the redesign of security architectures (Malatji et al., 2022). Cybersecurity governance maturity serves as the complementary capability that determines whether analytical insights are actually seized and transformed into coordinated action; mature governance clarifies accountability, decision rights, escalation paths, and business–security alignment. Because IT and business managers often interpret cyber resilience differently and create inconsistent priorities (Bagheri et al., 2023), mature governance reduces fragmentation and should amplify the positive effect of business analytics capability on cyber resilience. In sum, Dynamic Capabilities Theory unifies the model: analytics supplies adaptive analytical capacity, risk detection operationalizes threat sensing, governance maturity enables coherent seizing and transformation, and cyber resilience reflects the resulting ability to withstand, recover, learn, and adapt. Therefore, the study assumes that cyber threats generate the environmental dynamism that forces organizations to renew rather than merely deploy security resources, so stronger analytics and detection should raise resilience especially when mature governance permits rapid, coherent organizational action.

2.2.2. Organizational Information Processing Theory

Organizational Information Processing Theory, first advanced by Galbraith (1974) and later refined by Tushman & Nadler (1978), views organizations as information-processing systems that must match environmental uncertainty and resulting information demands with adequate processing capacity. Greater task uncertainty raises the volume of information that must be gathered, interpreted, and shared if performance is to remain acceptable (Galbraith, 1974), while effectiveness hinges on aligning those demands with the organization's capacity to meet them (Tushman & Nadler, 1978). When uncertainty rises, decision-makers need more timely, accurate, integrated, and interpretable information; firms can build this capacity through analytical tools, integrated databases, lateral communication, specialized roles, and formal coordination mechanisms. Recent work confirms the theory's usefulness in data-rich settings by showing that big-data analytics capability improves information integration and operational flexibility under disruption (Yu et al., 2021), making the perspective especially apt for cybersecurity contexts marked by high-volume data, ambiguous threat signals, fast-changing attack methods, and tight interdependence between technical and organizational units. Within this lens, business analytics capability functions as an expanded information-processing capacity that combines data quality, integrated infrastructure, analytical technologies, technical skill, managerial insight, and evidence-based decision routines. Because cybersecurity data are typically scattered across devices, applications, networks, departments, and external intelligence sources, mere data accumulation is insufficient without the ability to separate meaningful warnings from routine activity; value therefore depends on orchestrating technological, human, and organizational resources rather than volume alone (Mikalef et al., 2019). In this model, analytics enables firms to consolidate fragmented security information, detect relationships among events, anticipate consequences, and convey evidence to decision-makers, thereby supporting faster and better-informed preparation, response, recovery, and adaptation that strengthen cyber resilience. Data-driven risk detection serves as the core mechanism that turns raw security data into risk-relevant interpretations through continuous monitoring, pattern recognition, anomaly analysis, and predictive assessment, reducing ambiguity by distinguishing harmless variations from genuine vulnerabilities and emerging attacks. Evidence from SMEs shows that cybersecurity resilience includes the capacity to manage potential incidents, restore operations, and adapt to future threats (Fernandez de Arroyabe et al., 2024), and timely detection supplies the situational awareness needed across these stages by allowing isolation of compromised assets, prioritization of critical services, coordination of response teams, and preservation of continuity, while post-incident analysis further supports learning and procedural improvement. Cybersecurity governance maturity supplies the structural conditions that align processing capacity with cybersecurity demands; analytical insights cannot enhance resilience when information stays locked in technical units, escalation

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

paths are unclear, or managers cannot convert cyber indicators into business priorities. Mature governance establishes reporting relationships, information-sharing protocols, decision authority, risk thresholds, and accountability, linking technical intelligence to strategic judgments about continuity, stakeholder impact, and resource allocation. This integration matters because cyber resilience requires shared understanding between IT and business managers (Bagheri et al., 2023), so governance maturity should intensify the positive effect of business analytics capability on organizational cyber resilience. Overall, the theory accounts for the proposed framework through information-processing fit: cyber threats raise information requirements, analytics expands processing capacity, risk detection converts data into actionable intelligence, and mature governance ensures that intelligence is shared, interpreted, and translated into coordinated decisions. The study, therefore, assumes that evolving cyber threats heighten uncertainty and information needs; business analytics capability expands the ability to acquire, integrate, and interpret security data; data-driven risk detection reduces ambiguity by turning those data into actionable warnings; and cybersecurity governance maturity aligns information flows, decision rights, and response responsibilities, so that cyber resilience improves when analytical capacity matches threat-related information demands and governance ensures insights produce timely, coordinated decisions and learning.

2.3. The Impact of Business Analytics Capability

Business Analytics Capability (BAC) denotes a firm's capacity to mobilize and combine high-quality data, analytical technologies, technical expertise, managerial skills, and data-driven routines so as to produce actionable insights that guide organizational decisions. Therefore, it extends well beyond ownership of analytics software, constituting instead an organizational ability to orchestrate technological, human, and intangible resources (Mikalef et al., 2019; Huynh et al., 2023). BAC matters strategically because it converts scattered and complex data into knowledge that sharpens environmental sensing, forecasting, resource allocation, and coordinated decision-making. Organizational Information Processing Theory positions analytics as a means of expanding the capacity needed to interpret uncertainty and respond to information-intensive disruptions (Dubey et al., 2021), while Dynamic Capabilities Theory casts BAC as support for sensing emerging threats, selecting responses, and reconfiguring resources (Mikalef et al., 2020). Philosophically, BAC embodies a pragmatic stance toward knowledge in which analytical information gains value only when it yields actionable consequences rather than mere description (Goldkuhl, 2012), and it rests on a socio-technical ontology because capability arises from the interplay of data, technologies, employees, managerial judgment, and organizational routines. Consequently, BAC cannot be reduced to a stand-alone technological asset; its significance resides in the collective capacity to transform data into timely, contextually suitable actions. Higher levels of BAC should enhance organizational cyber resilience by helping firms detect cyber-risk patterns, anticipate vulnerabilities, assess incident impacts, and prioritize response resources. With stronger BAC, organizations can integrate network logs, user behavior, vulnerability reports, and external threat intelligence, thereby heightening situational awareness before, during, and after incidents and supporting swifter identification, containment, recovery, and learning. Although direct evidence concerning cyber resilience remains limited, related resilience research provides strong theoretical and empirical support. Dubey et al. (2021) found that data analytics capability complemented organizational flexibility to strengthen supply-chain resilience. Similarly, Bahrami & Shokouhyar (2022) showed that analytics capability enhanced resilience by improving information quality and innovation. More recently, Lin et al. (2025) demonstrated that big-data analytics capability increased both proactive and reactive organizational resilience, particularly under conditions of high environmental dynamism. The literature nevertheless remains nuanced. Some work suggests a robust effect because analytics markedly expands sensing, prediction, and response capacity under uncertainty (Dubey et al., 2021; Lin et al., 2025), yet systematic reviews indicate that BAC is conceptually fragmented and creates value through varied resource combinations and intermediate capabilities rather than a uniformly strong direct path (Huynh et al., 2023). Mikalef et al. (2020) likewise show that analytics capability influences competitive outcomes mainly through dynamic and operational capabilities, so its impact may prove neutral or weak when data quality is low, skills are lacking, insights fail to enter routines, or governance blocks timely action. From a critical-realist standpoint, BAC constitutes an underlying causal mechanism whose observable effects hinge on contextual structures and enabling conditions rather than automatic technological results (Mingers, 2015). Even so, because BAC systematically improves threat interpretation, decision speed, and adaptive resource coordination, its overall influence on cyber resilience should remain positive. Therefore:

H1: Business analytics capability has a positive impact on organizational cyber resilience.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

2.4. The Impact of Data Analytics Maturity

Data-Driven Risk Detection (DDRD) denotes an organization's ability to continuously gather, integrate, and analyze internal and external security data to identify anomalies, vulnerabilities, malicious activity, and emerging cyber threats in a timely manner (Sarker et al., 2020; Saeed et al., 2023). It combines security logs, network traffic, user behavior, cyber-threat intelligence, machine learning, and predictive techniques to transform fragmented security data into prioritized and actionable risk warnings (Ferrag et al., 2020; Saeed et al., 2023; Sarker et al., 2020). Unlike conventional rule-based systems, DDRD can detect complex patterns and previously unseen behaviors across large, fast-changing datasets (Sarker et al., 2020). Its value rests in shortening the interval between threat appearance, organizational recognition, and defensive response. Cyber-threat intelligence further bolsters precautionary decisions by furnishing contextual knowledge of attackers, vulnerabilities, and probable attack paths (Saeed et al., 2023). Viewed through Organizational Information Processing Theory, DDRD lowers uncertainty and equivocality by raising the timeliness, accuracy, and interpretability of risk information (Yu et al., 2021). Epistemologically it begins with a positivist stance that treats observable digital traces as sources of regularities and threat estimates (Sarker et al., 2020), yet a critical-realist reading is more fitting because cyber risks exist independently of detection systems(Mingers, 2015) while their indicators remain incomplete, context-bound, and open to manipulation (Korycki & Krawczyk, 2023); DDRD, therefore, yields evidence-informed risk judgments rather than perfectly objective portraits of cyber reality.

Stronger DDRD should raise organizational cyber resilience by sharpening anticipation, containment, recovery, and adaptation. Continuous monitoring and anomaly detection let firms identify compromised accounts, abnormal traffic, malware behavior, and unauthorized access earlier, thereby cutting attacker dwell time and allowing security teams to isolate affected resources before disruption spreads across interconnected systems. Machine-learning and deep-learning techniques can enhance intrusion detection by capturing complex relationships that traditional security rules may miss (Ferrag et al., 2020). DDRD also aids recovery by pinpointing compromised assets and reconstructing attack sequences, while post-incident analysis generates knowledge for refining controls and response routines. Systematic reviews show that artificial intelligence strengthens cybersecurity through automated monitoring, threat classification, and quicker response (Jada & Mayayise, 2024), and cyber-threat intelligence can likewise build organizational resilience by supporting proactive preparation and informed coordination (Saeed et al., 2023). The size of this effect, however, remains debated. A strong-effect view holds that advanced analytics markedly improve the speed, scale, and accuracy of threat recognition, enabling organizations to act before incidents escalate into operational crises (Sarker et al., 2020; Ferrag et al., 2020). A more contingent view counters that detection technologies do not automatically produce resilience; their contribution can be undermined by imbalanced or outdated datasets, false positives, model opacity, shifting attack patterns, and weak integration with incident-response processes. Models trained on historical data may falter against novel threats or concept drift, and adversarial manipulation can deliberately distort classifications (Korycki & Krawczyk, 2023). Jada & Mayayise (2024) likewise identify data-quality issues, adversarial attacks, and organizational readiness as factors that shape the cybersecurity value of artificial intelligence. From a pragmatic standpoint, DDRD should be judged by whether its warnings enable effective action rather than by statistical accuracy alone. Although its impact depends on human judgment, governance, and response capacity, DDRD still improves situational awareness and permits earlier intervention, so a positive overall relationship with cyber resilience is expected. Accordingly:

H2: Data-driven risk detection has a positive impact on organizational cyber resilience.

2.5 The Moderating Role of Cybersecurity Governance Maturity

Cybersecurity governance maturity (CGM) refers to the extent to which an organization has institutionalized, integrated, assessed, and continuously improved its cybersecurity governance structures, policies, decision authority, accountability mechanisms, risk management processes, and oversight practices (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025; Rabii et al., 2020). It extends beyond the mere existence of cybersecurity policies by reflecting how consistently cybersecurity responsibilities and decision-making processes are embedded across strategic, managerial, and operational levels (Bagheri et al., 2023; Büyüközkan & Güler, 2025). Mature governance clarifies risk ownership, aligns cybersecurity with organizational goals, establishes reporting and escalation procedures, allocates resources, evaluates control effectiveness, and incorporates incident learning into future decisions. Therefore, cybersecurity maturity models assess progressive development across technological, organizational, human, and governance aspects rather than viewing security as a binary condition (Rabii et al., 2020; Büyüközkan & Güler, 2025). Their

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

importance lies in helping organizations diagnose vulnerabilities, prioritize investments, and develop repeatable practices to support business continuity and security resilience (Brezavšček & Baggia, 2025).

Philosophically, CGM encompasses both ethical and consequential foundations. From an ethical standpoint, governance represents an organization's obligation to establish accountability, protect stakeholder information, and exercise responsible oversight regardless of whether incidents occur. From a consequential perspective, its value is assessed based on whether governance reduces disruption, accelerates recovery, and protects organizational value. Critical realism provides further clarification because governance constitutes a fundamental organizational mechanism whose impact manifests through decision-making, coordination, resource allocation, and disciplined action, not merely through policy documentation (Mingers, 2015). Therefore, maturity should demonstrate governance in action, not symbolic compliance.

CGM is expected to positively regulate the relationship between business analytics capabilities and organizational cybersecurity resilience. Business analytics can identify anomalies, estimate vulnerabilities, and generate risk intelligence, but these insights cannot enhance resilience unless organizations identify who receives them, who authorizes action, and how resources are mobilized. Under mature governance, analytical outcomes are linked to risk thresholds, escalation pathways, incident response responsibilities, board oversight, and recovery priorities. Consequently, data analytics becomes more useful, enabling organizations to predict threats, coordinate responses, preserve critical operations, and learn from incidents. Evidence showing that IT governance agreements are related to cybersecurity breach outcomes supports the importance of governance structures in transforming technical resources into organizational protection (Lankton et al., 2021). Research on maturity levels also highlights that structured assessments and continuous improvement strengthen cybersecurity readiness and resilience (Büyüközkan & Güler, 2025).

Therefore, the strong impact perspective suggests that CGM significantly amplifies the relationship between data analytics and resilience by preventing analytical intelligence from being isolated within technical departments. However, a neutral or conditional perspective may also be justified. Governance frameworks can become compliance exercises that increase documentation without improving adaptive action. Research on cyber risk reveals significant heterogeneity in measurement, data availability, and organizational implementation, limiting the assumption that formal governance automatically produces effective outcomes (Cremer et al., 2022). Furthermore, Tsen et al. (2025) found that higher cyber resilience is associated with several aspects of preparedness but does not necessarily mitigate post-incident consequences. Accordingly, direct evidence for the proposed moderation remains limited, and the level of governance maturity may have little influence when leadership involvement, analytical capacity, information quality, or response resources are inadequate. However, because mature governance combines analytical insights with authority, accountability, and coordinated action, a positive moderation effect is theoretically expected. Accordingly, H3 is as follows:

H3: Cybersecurity governance maturity positively moderates the relationship between business analytics capability and organizational cyber resilience.

Drawing on established theoretical foundations, this study proposes the conceptual framework presented in Figure 1 to advance and enrich the existing body of knowledge:

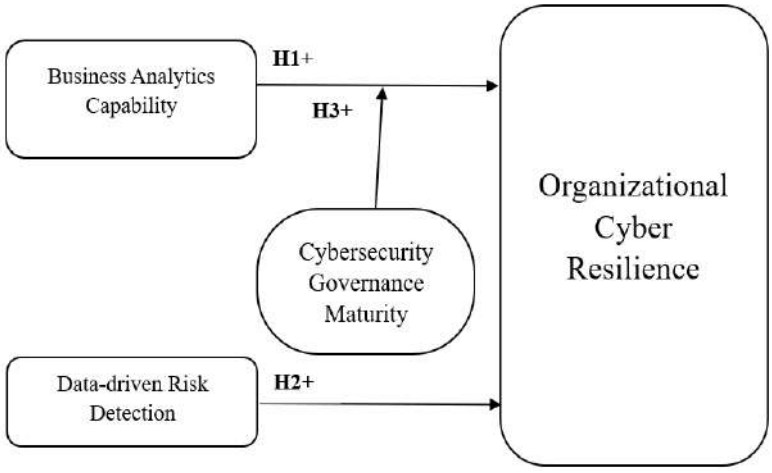

Figure 1: The Paper Conceptual Framework

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

3. METHODS

3.1. Sampling Strategy

This study adopted a quantitative cross-sectional design to investigate how business analytics capability and data-driven risk detection influence organizational cyber resilience, while also exploring the moderating influence of cybersecurity governance maturity. The quantitative method proved suitable as it supported rigorous hypothesis testing and statistical estimation of both direct and interaction effects through standardized survey responses. By employing a cross-sectional approach, the research efficiently captured participants' perceptions of organizational analytics practices, cyber-risk detection mechanisms, governance arrangements, and resilience at a single point in time (Bryman, 2016).

A purposive sampling strategy was chosen to ensure that respondents possessed relevant professional knowledge or experience, with the individual organizational member serving as the unit of analysis even though the constructs themselves were evaluated at the organizational level via informed perceptions. Eligible participants encompassed senior and middle managers, cybersecurity and IT specialists, business and data analysts, risk-management staff, and employees engaged in digital operations or continuity planning; these individuals were drawn from organizations that rely on digital information systems and face cybersecurity threats. Deliberate efforts were made to include respondents from varied roles, industries, and firm sizes in order to enhance sample diversity and lessen over-reliance on any single professional category.

Data collection relied on a structured, self-administered questionnaire adapted from established scholarly sources. Items measuring business analytics capability evaluated the organization's capacity to integrate reliable data, analytical infrastructure, technical expertise, managerial competence, and data-driven decision routines (Mikalef et al., 2019; Huynh et al., 2023). Data-driven risk detection captured continuous monitoring, data integration, anomaly recognition, threat identification, and the generation of actionable risk alerts (Sarker et al., 2020; Saeed et al., 2023). Cybersecurity governance maturity reflected the institutionalization of policies, accountability structures, decision authority, risk oversight, reporting procedures, and continuous improvement practices (Rabii et al., 2020; Büyüközkan & Güler, 2025). Organizational cyber resilience assessed the ability to anticipate, absorb, respond to, recover from, and adapt after cyber incidents while maintaining essential operations (Fernandez de Arroyabe et al., 2024; Tzavara & Vassiliadis, 2024).

All items employed a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Prior to the main survey, academic experts and practitioners in business analytics, cybersecurity, risk management, and organizational governance reviewed the instrument to confirm content validity and clarity; a subsequent pilot test with eligible respondents led to minor wording adjustments. The finalized questionnaire was distributed electronically via professional networks, organizational contacts, industry groups, and online platforms. Participation remained voluntary, respondents were informed of the study's academic purpose, and confidentiality was guaranteed. After exclusion of incomplete, duplicate, and patterned responses, 385 valid questionnaires were retained—a sample size that surpassed conventional thresholds for multivariate analysis (Hair et al., 2009), although suitability for moderated regression should also be verified through statistical power analysis rather than sample size alone.

3.2. Data analysis

Data analysis proceeded sequentially with IBM SPSS and Hayes' Process macro. Descriptive statistics first summarized demographic and professional characteristics. Cronbach's alpha then evaluated the internal consistency of business analytics capability, data-driven risk detection, cybersecurity governance maturity, and organizational cyber resilience; constructs meeting or exceeding an alpha of 0.70 and corrected item–total correlations above 0.30 were judged reliable (Tavakol & Dennick, 2011). Exploratory factor analysis using principal component analysis with Varimax rotation next examined the empirical structure of the measurement items. Items were retained when primary loadings exceeded 0.50 and problematic cross-loadings were absent (Hair et al., 2009). Multiple linear regression subsequently tested the direct effects of business analytics capability and data-driven risk detection on organizational cyber resilience (Shrestha, 2020). Significance was determined at the 5% level. Finally, Hayes' Process macro-Model 1 examined whether cybersecurity governance maturity moderated the relationship between business analytics capability and organizational cyber resilience (Hayes, 2022).

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

4. RESULTS

4.1. Descriptive Statistical Analysis

The sample reflected organizations operating across the principal economic regions of Vietnam. Specifically, 44.4% of respondents worked for organizations in Southern Vietnam, 31.9% were based in Northern Vietnam, and 23.6% worked in Central Vietnam. Regarding organizational roles, middle or functional managers represented the largest group at 24.9%, followed by owners, directors, or senior managers at 21.8%. Cybersecurity or information technology specialists accounted for 20.5%, while business or data analytics professionals comprised 17.7%. Risk management, compliance, digital operations, or business continuity personnel constituted the remaining 15.1%. In terms of organizational size, organizations employing 50 to 249 people formed the largest category at 33.5%, followed by those with 250 to 999 employees at 30.1%. Large organizations with at least 1,000 employees represented 20.3%, whereas organizations with fewer than 50 employees accounted for 16.1%. Furthermore, 37.7% of participants reported high familiarity with their organizations' analytics capabilities, cyber-risk detection practices, cybersecurity governance, and resilience arrangements. Another 21.0% indicated very high familiarity, while 30.9% reported moderate familiarity. Only 10.4% demonstrated limited familiarity. Overall, the sample covered diverse organizational contexts, and most respondents possessed sufficient professional knowledge to provide informed assessments of the study constructs.

4.2. Reliability analysis

Table 1 outlines the measurement items employed to operationalize the study constructs. Each construct consisted of four items adapted from established academic sources to ensure theoretical alignment and comprehensive representation of its key dimensions. Respondents evaluated all items using a five-point Likert scale ranging from 1, strongly disagree, to 5, strongly agree.

Table 1: Measurement Items

Code	Survey item	Theoretical source
Organizational Cyber Resilience		
OCR1	Our organization regularly prepares for potential cyber incidents.	(Tzavara & Vassiliadis, 2024; Fernandez de Arroyabe et al., 2024)
OCR2	Our organization can maintain its essential operations during a cyber incident.	(Malatji et al., 2022; Tzavara & Vassiliadis, 2024)
OCR3	Our organization can restore its essential operations following a cyber incident.	(Fernandez de Arroyabe et al., 2024; Tzavara & Vassiliadis, 2024)
OCR4	Our organization revises its cybersecurity practices based on lessons learned from cyber incidents.	(Dupont et al., 2023; Goel et al., 2023)
Business Analytics Capability		
BAC1	Our organization integrates data from relevant internal and external sources for analytical purposes.	(Mikalef et al., 2019; Huynh et al., 2023)
BAC2	Our organization has appropriate technological infrastructure for conducting business analytics.	(Mikalef et al., 2019; Huynh et al., 2023)
BAC3	Employees responsible for analytics possess the expertise required to interpret analytical outputs.	(Mikalef et al., 2019; Mikalef et al., 2020)
BAC4	Managers in our organization regularly incorporate analytical information into decision-making routines.	(Mikalef et al., 2019; Mikalef et al., 2021)
Data-Driven Risk Detection		

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

DDRD1	Our organization continuously monitors digital activity for signs of potential cyber risks.	(Sarker et al., 2020; Saeed et al., 2023)
DDRD2	Our organization combines data from multiple security-related sources when assessing cyber risks.	(Sarker et al., 2020; Saeed et al., 2023)
DDRD3	Our organization uses data analysis to identify unusual patterns in its digital systems.	(Ferrag et al., 2020; Sarker et al., 2020)
DDRD4	Our organization generates prioritized risk alerts from its cybersecurity data.	(Saeed et al., 2023; Jada & Mayayise, 2024)
Cybersecurity Governance Maturity		
CGM1	Our organization has formally established cybersecurity policies that are consistently implemented.	(Rabii et al., 2020; Büyüközkan & Güler, 2025)
CGM2	Responsibility for cybersecurity decisions is clearly assigned within our organization.	(Lankton et al., 2021; Büyüközkan & Güler, 2025)
CGM3	Our organization has established reporting procedures for escalating cybersecurity risks.	(Rabii et al., 2020; Brezavšček & Baggia, 2025)
CGM4	Our organization periodically reviews its cybersecurity governance practices for continuous improvement.	(Rabii et al., 2020; Büyüközkan & Güler, 2025)

Table 2: Reliability analysis of "Organizational Cyber Resilience".

Reliability Statistics

Cronbach's Alpha	N of Items
.732	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
OCR1	11.124	4.382	0.426	0.728
OCR2	11.267	4.196	0.417	0.730
OCR3	11.058	4.451	0.442	0.719
OCR4	11.196	4.273	0.468	0.707

Source: (The authors, 2026)

As shown in Table 2, the four items yielded corrected item-total correlations between 0.417 and 0.468, all above the suggested cutoff of 0.30. The complete scale produced a Cronbach's alpha of 0.732, which exceeded the conventional minimum of 0.70 and thereby demonstrated adequate internal consistency. In addition, the alpha coefficients calculated after successive item deletion fell between 0.707 and 0.730 and stayed below the overall value, confirming that the exclusion of any single item would weaken scale reliability. Consequently, ocr1 through ocr4 made substantive contributions to the assessment of organizational cyber resilience and were kept for later analyses. Similar reliability estimates appeared for the remaining measurement scales employed in the research (Hair et al., 2009; Tavakol & Dennick, 2011).

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

4.3. Exploratory factor analysis (EFA)

Table 3: Factor Loading Matrix.

Rotated Component Matrix[a]							
Component with loading factors							
1		2		3		4	
BAC1	0.781	DDRD1	0.758	CGM1	0.774	OCR1	0.648
BAC2	0.824	DDRD2	0.803	CGM2	0.817	OCR2	0.632
BAC3	0.746	DDRD3	0.729	CGM3	0.752	OCR3	0.671
BAC4	0.793	DDRD4	0.786	CGM4	0.798	OCR4	0.706
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.							
a. Rotation converged in 7 iterations.							

Source: (The authors, 2026)

Table 3 displays the outcomes of the exploratory factor analysis and reveals four separate factors that correspond to business analytics capability, data driven risk detection, cybersecurity governance maturity, and organizational cyber resilience. Every one of the 16 measurement items loaded adequately onto the factors they were designed to represent, with loadings spanning 0.632 to 0.824 and thereby surpassing the accepted minimum of 0.50 (Hair et al., 2009). After six iterations the Varimax rotation reached convergence and confirmed that the factor solution remained stable. As a result, none of the items needed to be discarded and the full set of 16 indicators was kept for further statistical work. In summary, these results offer solid support for the hypothesized four factor structure as well as for the construct validity of the measurement model.

4.4. Multiple linear regression model

Table 4: Coefficients[a].

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
Constant	0.294	0.126		2.333	0.020
BAC	0.438	0.027	0.573	16.222	0.000
DDRD	0.491	0.025	0.638	19.640	0.000
a. Dependent Variable: OCR					

Source: (The authors, 2026)

Where BAC represents the mean of BAC1 to BAC4, DDRD represents the mean of DDRD1 to DDRD4, and OCR represents the mean of OCR1 to OCR4.

As shown in Table 4, the significance values for the relationships between business analytics capability and organizational cyber resilience and between data-driven risk detection and organizational cyber resilience were both below 0.001, which is well below the 0.05 threshold. Business analytics capability had a significant positive effect on organizational cyber resilience, with $\beta = 0.573$, $t = 16.222$, and $p < 0.001$. Data-driven risk detection also exerted a significant positive effect, with $\beta = 0.638$, $t = 19.640$, and $p < 0.001$. These findings provide strong empirical support for accepting H1 and H2.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

4.5. Moderator analysis

Table 5: Results analysis of "Cybersecurity Governance Maturity".

Model: 1 Y: OCR X: BAC W: CGM Sample Size: 385

****

OUTCOME VARIABLE: OCR Model Summary

R	R-sq	MSE	F	dl1	dl2	p
.691	.477	0.312	115.828	3.000	381.000	.000

Model

	Coeff.	SE	t	p	LLCI	ULCI
Constant	3.218	0.041	78.488	0.000	3.137	3.299
BAC	0.589	0.046	12.804	0.000	0.499	0.679
CGM	0.625	0.044	14.205	0.000	0.539	0.711
Int_1	0.407	0.039	10.436	0.000	0.330	0.484

Source: (The authors, 2026)

Where CGM was calculated as the mean score of items CGM1 to CGM4.

The positive interaction coefficient of B = 0.407 shows that greater cybersecurity governance maturity amplifies the favorable influence of business analytics capability on organizational cyber resilience. While business analytics capability helps organizations combine data, detect patterns, make sense of cyber risk information, and guide decisions grounded in evidence, this contribution grows more pronounced when mature cybersecurity governance structures are in place. Clear responsibility assignments, formal reporting channels, defined escalation pathways, ongoing governance evaluations, and steady policy application enable decision makers to examine analytical findings with greater care and convert them into aligned cybersecurity measures. As a result, organizations that possess mature cybersecurity governance can apply analytical insights more productively to foresee cyber threats, sustain core operations, organize incident responses, facilitate recovery, and refine cybersecurity practices following incidents. In addition, the confidence interval for the interaction term runs from LLCI = 0.330 to ULCI = 0.484 and does not contain zero, thereby verifying the significance and robustness of this positive moderating influence. Collectively, the results position cybersecurity governance maturity as a key boundary condition that heightens the positive role of business analytics capability in fostering organizational cyber resilience and, thus, offer empirical backing for hypothesis H3.

5. DISCUSSION

5.1. Result Summary

Business analytics capability and data-driven risk detection each exert significant positive influences on organizational cyber resilience as reflected in their standardized regression coefficients of 0.573 and 0.638 respectively. These results demonstrate that integrated analytical resources and timely risk intelligence help organizations recognize emerging threats interpret complex security information coordinate incident responses maintain essential operations and recover more effectively from cyber disruptions. Data-driven risk detection produces the stronger direct effect emphasizing the importance of continuous monitoring anomaly identification and prioritized cyber risk alerts. At the same time, cybersecurity governance maturity functions as a significant positive moderator that strengthens the relationship between business analytics capability and organizational cyber resilience as confirmed by the interaction coefficient of 0.407 and its confidence interval ranging from 0.330 to 0.484. This pattern indicates that analytics generates greater resilience benefits when supported by clearly assigned responsibilities formal reporting procedures established escalation mechanisms consistent policy implementation and continuous governance improvement. In summary, the empirical evidence supports all three hypotheses and confirms the proposed theoretical framework connecting business analytics capability data-driven risk detection cybersecurity governance maturity and organizational cyber resilience.

Regarding the first research question the findings verify that business analytics capability significantly enhances organizational cyber resilience. The second research question is addressed by establishing that data-driven risk detection also produces a significant positive effect and has a moderately stronger standardized influence than business analytics capability. The third research question is answered by demonstrating that higher cybersecurity governance maturity meaningfully amplifies the positive contribution of

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

business analytics capability to organizational cyber resilience. To sum up, these findings suggest that organizations achieve stronger cyber resilience when they combine advanced analytical capabilities with continuous risk detection and mature governance structures. Strengthening cyber resilience therefore requires organizations to integrate reliable security data develop analytical expertise continuously monitor digital activity establish clear decision authority maintain effective escalation procedures and regularly improve cybersecurity governance practices.

5.2. Theoretical Implications

The empirical findings strongly support H1 as business analytics capability significantly improves organizational cyber resilience with β = 0.573. This result strongly concurs with Dubey et al. (2021) who associate analytics capability with resilience through enhanced information processing and organizational flexibility and Lin et al. (2025) who demonstrate its contribution to proactive and reactive resilience. It also supports Mikalef et al. (2020) although their argument that analytics primarily creates value through dynamic and operational capabilities suggests a less direct relationship. Accordingly, this study is not in favor of technological determinism whereby acquiring analytical technologies automatically produces resilience. Instead, it concurs with Huynh et al. (2023) that analytics capability depends on coordinated combinations of data infrastructure expertise and managerial routines. The substantial coefficient indicates that analytics becomes resilience enhancing when organizations can convert fragmented cyber information into actionable knowledge and adaptive responses. Theoretically, this research extends Dynamic Capabilities Theory by identifying business analytics capability as a mechanism supporting threat sensing response selection and resource reconfiguration. It also advances Organizational Information Processing Theory by showing that analytical capacity helps organizations match escalating cyber uncertainty with integrated and interpretable information.

The findings strongly support H2 with data driven risk detection producing a significant positive effect on organizational cyber resilience at β = 0.638. This result strongly concurs with Sarker et al. (2020) who argue that cybersecurity analytics can identify complex and previously unseen behavioral patterns and Saeed et al. (2023) who emphasize the role of cyber threat intelligence in contextualizing vulnerabilities and likely attack paths. The stronger coefficient relative to business analytics capability suggests that converting data into timely warnings may be more immediately consequential for resilience than possessing broader analytical resources. Nevertheless, this study only partially concurs with optimistic claims that increasingly sophisticated detection necessarily ensures effective protection. Ferrag et al. (2020) demonstrate the detection potential of advanced learning techniques whereas Korycki & Krawczyk (2023) warn that concept drift and adversarial manipulation can undermine model accuracy. Jada & Mayayise (2024) similarly highlight data quality and organizational readiness constraints. Theoretically this research advances Organizational Information Processing Theory by positioning data driven risk detection as a threat specific sensing mechanism that reduces ambiguity and transforms dispersed security data into prioritized intelligence. It further refines Dynamic Capabilities Theory by demonstrating that resilience begins with actionable sensing rather than passive data accumulation.

The findings strongly support H3 as the positive interaction coefficient of B = 0.407 indicates that cybersecurity governance maturity strengthens the relationship between business analytics capability and organizational cyber resilience. This outcome strongly concurs with Lankton et al. (2021) whose findings connect IT governance arrangements with cybersecurity outcomes and Büyüközkan & Güler (2025) who view maturity as progressive institutionalization across technological organizational and human dimensions. It also supports Bagheri et al. (2023) who argue that fragmented interpretations between business and IT managers weaken coordinated cyber resilience decisions. However, the study is not in favor of assuming that formal policies alone represent effective governance. Cremer et al. (2022) expose substantial heterogeneity in cyber risk measurement and implementation while Tsen et al. (2025) show that greater preparedness does not necessarily reduce post incident consequences. Therefore, the significant moderation implies that governance matters when it actively connects analytical intelligence with accountability escalation authority resource mobilization and organizational learning. Theoretically, this study contributes by identifying cybersecurity governance maturity as a boundary condition within Dynamic Capabilities Theory and as an information processing alignment mechanism that determines whether analytical capacity is translated into coordinated resilience outcomes.

5.3. Practical Implications

The significant effect of business analytics capability on organizational cyber resilience with β = 0.573 indicates that managers should treat analytics as an integrated organizational capability rather than merely an investment in software. Organizations should combine reliable cybersecurity data, compatible analytical infrastructure, skilled analysts, managerial interpretation, and data driven

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

decision routines. This requires integrating network logs, vulnerability reports, user activity, and external threat information into accessible dashboards while providing managers with training in interpreting analytical results. Cross functional teams involving cybersecurity, analytics, operations, and senior management should regularly review threat patterns and translate them into response priorities. Such resource orchestration is important because different configurations of technological, human, and organizational resources generate different levels of value from analytics (Mikalef et al., 2019). Organizations should, therefore, assess analytics by whether it strengthens anticipation, containment, recovery, and learning rather than by the volume of collected data or sophistication of acquired technologies.

The stronger effect of data driven risk detection with $\beta = 0.638$ suggests that organizations should prioritize mechanisms that transform security data into timely and actionable warnings. Managers should implement continuous monitoring, integrate internal security records with external threat intelligence, and establish risk scoring procedures that distinguish critical anomalies from routine variations. Alerts should be prioritized according to threat severity, asset importance, and potential operational consequences to reduce alert fatigue. Security teams should also periodically validate detection models using new incident data because shifting attack patterns can reduce the relevance of historical indicators. Cyber threat intelligence supports resilience when organizations systematically acquire, process, evaluate, and disseminate threat information (Saeed et al., 2023). Accordingly, detection performance should not be judged solely through technical accuracy. Managers should also monitor response time, false alert rates, containment speed, service continuity, and lessons incorporated following incidents.

The positive moderation coefficient of $B = 0.407$ demonstrates that business analytics produces greater resilience benefits under mature cybersecurity governance. Organizations should formally assign cyber risk ownership, define reporting relationships, establish escalation thresholds, and specify who may authorize containment and recovery actions. Boards and senior managers should periodically review risk dashboards, response performance, unresolved vulnerabilities, and lessons from simulations or actual incidents. This is essential because managerial and technical personnel can interpret cyber resilience differently, thereby fragmenting priorities and responses (Bagheri et al., 2023). Organizations should use maturity assessments to identify governance weaknesses, but they should avoid treating maturity models as compliance checklists because existing models remain diverse and insufficiently convergent (Rabii et al., 2020). Instead, governance maturity should be demonstrated through consistent implementation, rapid analytical escalation, accountable decisions, tested response procedures, and continuous improvement.

5.4. Limitations

This study's cross sectional design captures perceptions at one point in time and, thus, cannot establish definitive causal or temporal relationships among analytics capability, risk detection, governance maturity, and cyber resilience. Purposive sampling and reliance on 385 self-reported responses may introduce selection bias, common method variance, and socially desirable assessments of cybersecurity preparedness. Although participants possessed relevant professional knowledge, individual perceptions may not fully represent organization level capabilities or actual incident performance. The study also combines organizations from different industries and sizes, potentially concealing sector specific risk environments. Finally, the model examines only one moderator and does not account for leadership commitment, cybersecurity culture, resource availability, regulatory pressure, attack severity, or prior incident experience.

5.5. Future Research Directions

Future research should employ longitudinal or panel designs to determine how analytical capabilities and governance maturity shape resilience before, during, and after cyber incidents. Combining surveys with objective evidence including incident records, recovery times, false alert rates, system downtime, and audit findings would reduce common method bias and strengthen causal interpretation. Multi informant studies could compare assessments from senior managers, cybersecurity specialists, analysts, and operational employees. Researchers should also test the framework across industries, organizational sizes, and national regulatory environments through multigroup analysis. Experimental or scenario-based research could examine whether different governance arrangements change how managers respond to identical analytical warnings. Further models should investigate cybersecurity culture, leadership commitment, analytical talent, environmental turbulence, and incident severity as mediators, moderators, or boundary conditions.

5.6. Conclusion

This study demonstrates that business analytics capability and data-driven risk detection significantly strengthen organizational cyber resilience, with data-driven risk detection producing the stronger direct influence. Cybersecurity governance maturity, further,

intensifies the contribution of analytics capability, confirming that analytical resources create greater value when supported by accountability, escalation authority, structured oversight, and continuous improvement. The findings support all three hypotheses and integrate Dynamic Capabilities Theory with Organizational Information Processing Theory by showing how organizations sense threats, interpret complex security information, coordinate responses, and reconfigure resources. Overall, cyber resilience does not arise from technological investment alone. It depends on the coordinated combination of analytical capacity, actionable threat detection, and mature governance. Therefore, organizations seeking sustained operational continuity should develop these capabilities jointly rather than pursuing isolated cybersecurity initiatives.

REFERENCES

1. Al-Ghattas, H., & Marjanovic, O. (2021, January). Business analytics capabilities for organisational resilience. In *Hawaii International Conference on System Sciences (54th: 2021)* (pp. 228–235). University of Hawaii at Manoa. https://doi.org/10.24251/hicss.2021.026
2. Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering, 149*, 106829. https://doi.org/10.1016/j.cie.2020.106829
3. Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience: Management perspectives. *Australasian Journal of Information Systems, 27*. https://doi.org/10.3127/ajis.v27i0.4183
4. Bahrami, M., & Shokouhyar, S. (2022). The role of big data analytics capabilities in bolstering supply chain resilience and firm performance: A dynamic capability view. *Information Technology & People, 35*(5), 1621–1651. https://doi.org/10.1108/ITP-01-2021-0048
5. Brezavšček, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems, 13*(1), 52. https://doi.org/10.3390/systems13010052
6. Bryman, A. (2016). *Social research methods*. Oxford University Press.
7. Büyüközkan, G., & Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. *Technological Forecasting and Social Change, 213*, 123996. https://doi.org/10.1016/j.techfore.2025.123996
8. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance: Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6
9. Dubey, R., Gunasekaran, A., Childe, S. J., Fosso Wamba, S., Roubaud, D., & Foropon, C. (2021). Empirical investigation of data analytics capability and organizational flexibility as complements to supply chain resilience. *International Journal of Production Research, 59*(1), 110–128. https://doi.org/10.1080/00207543.2019.1582820
10. Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security, 132*, 103372. https://doi.org/10.1016/j.cose.2023.103372
11. Estay, D. A. S., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security, 97*, 101996. https://doi.org/10.1016/j.cose.2020.101996
12. Fernandez de Arroyabe, J. C., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. (2024). Cybersecurity resilience in SMEs: A machine learning approach. *Journal of Computer Information Systems, 64*(6), 711–727. https://doi.org/10.1080/08874417.2023.2248925
13. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419
14. Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces, 4*(3), 28–36. https://doi.org/10.1287/inte.4.3.28
15. Goel, L., Russell, D., Williamson, S., & Zhang, J. Z. (2023). Information systems security resilience as a dynamic capability. *Journal of Enterprise Information Management, 36*(4), 906–924. https://doi.org/10.1108/JEIM-07-2022-0228
16. Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems, 21*(2), 135–146. https://doi.org/10.1057/ejis.2011.54
17. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

18. Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (3rd ed.). Guilford Press.
19. Huynh, M. T., Nippa, M., & Aichner, T. (2023). Big data analytics capabilities: Patchwork or progress? A systematic review of the status quo and implications for future research. *Technological Forecasting and Social Change, 197*, 122884. https://doi.org/10.1016/j.techfore.2023.122884
20. Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063
21. Korycki, Ł., & Krawczyk, B. (2023). Adversarial concept drift detection under poisoning attacks for robust data stream mining. *Machine Learning, 112*(10), 4013–4048. https://doi.org/10.1007/s10994-022-06177-w
22. Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity breaches and the role of information technology governance in audit committee charters. *Journal of Information Systems, 35*(1), 101–119. https://doi.org/10.1108/ICS-03-2019-0036
23. Lin, J., Wu, S., & Luo, X. (2025). How does big data analytics capability affect firm performance? Unveiling the role of organisational resilience and environmental dynamism. *European Journal of Information Systems, 34*(3), 502–528. https://doi.org/10.1080/0960085X.2024.2375262
24. Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security, 30*(2), 255–279. https://doi.org/10.1108/ICS-06-2021-0091
25. Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2019). Big data analytics and firm performance: Findings from a mixed-method approach. *Journal of Business Research, 98*, 261–276. https://doi.org/10.1016/j.jbusres.2019.01.044
26. Mikalef, P., Krogstie, J., Pappas, I. O., & Pavlou, P. (2020). Exploring the relationship between big data analytics capability and competitive performance: The mediating roles of dynamic and operational capabilities. *Information & Management, 57*(2), 103169. https://doi.org/10.1016/j.im.2019.05.004
27. Mikalef, P., Van De Wetering, R., & Krogstie, J. (2021). Building dynamic capabilities by leveraging big data analytics: The role of organizational inertia. *Information & Management, 58*(6), 103412. https://doi.org/10.1016/j.im.2020.103412
28. Mingers, J. (2015). Helping business schools engage with real problems: The contribution of critical realism and systems thinking. *European Journal of Operational Research, 242*(1), 316–331. https://doi.org/10.1016/j.ejor.2014.10.058
29. Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information & Computer Security, 28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039
30. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273
31. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data, 7*(1), 41. https://doi.org/10.1186/s40537-020-00318-5
32. Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Pearson Education.
33. Shrestha, N. (2020). Detecting multicollinearity in regression analysis. *American Journal of Applied Mathematics and Statistics, 8*(2), 39–42. https://doi.org/10.12691/ajams-8-2-1
34. Shrestha, Y. R., Ben-Menahem, S. M., & Von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. *California Management Review, 61*(4), 66–83. https://doi.org/10.1177/0008125619862257
35. Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd
36. Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning, 51*(1), 40–49. https://doi.org/10.1016/j.lrp.2017.06.007
37. Tsen, E., Ko, R. K., & Slapničar, S. (2025). The effect of organizational cyber resilience on cyber incident outcomes. *Journal of Cybersecurity, 11*(1), tyaf040. https://doi.org/10.1093/cybsec/tyaf040
38. Tushman, M. L., & Nadler, D. A. (1978). Information processing as an integrating concept in organizational design. *Academy of Management Review, 3*(3), 613–624. https://doi.org/10.5465/amr.1978.4305791
39. Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security, 23*(3), 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 08 August 2026
DOI: 10.47191/ijcsrr/V9-i8-48, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

40. Yu, W., Zhao, G., Liu, Q., & Song, Y. (2021). Role of big data analytics capability in developing integrated hospital supply chains and operational flexibility: An organizational information processing theory perspective. *Technological Forecasting and Social Change, 163*, 120417. https://doi.org/10.1016/j.techfore.2020.120417

Cite this Article: Vinh, V.M., Thanh, M.L.B., Chi, L.P. (2026). Business Analytics Capability and Organizational Cyber Resilience: The Roles of Data-Driven Risk Detection and Cybersecurity Governance. International Journal of Current Science Research and Review, 9(8), pp. 4757-4772. DOI: https://doi.org/10.47191/ijcsrr/V9-i8-48