INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 14, Issue 4, (2024) E-ISSN: 2225-8329

Factors Affecting Cybersecurity Readiness from Dynamic Capabilities Perspective: A Thematic Review

Ahmad Fairuz Mohamed Noor, Sedigheh Moghavvemi, Farzana Parveen Tajudeen

Faculty of Business and Economics, Universiti Malaya, Kuala Lumpur, Malaysia

Corresponding Authors Email: sedigheh@um.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARAFMS/v14-i4/23970 DOI:10.6007/IJARAFMS/v14-i4/23970

Published Online: 25 December 2024

Abstract

As cyber threats become increasingly sophisticated, organizations worldwide face rising challenges across various industries, making proactive cybersecurity readiness essential. This study addresses a gap in the literature by analysing factors affecting cybersecurity readiness from 2014 to 2023, with a focus on the underutilized dynamic capabilities theory in the context of cybersecurity. Using a thematic literature review methodology, this research explores the key factors influencing organizational cybersecurity readiness. The study identifies critical factors that enhance cybersecurity readiness, categorized into three capabilities: sensing (detecting and adapting to threats), seizing (proactively managing risks), and transforming (continuously evolving security measures and organizational culture). It emphasizes the importance of effective resource allocation and dynamic leadership in fostering a strong cybersecurity posture. These factors are synthesized into a framework that offers a comprehensive understanding of cybersecurity readiness. This study provides new insights into the application of dynamic capabilities theory to cybersecurity, offering a novel approach to improving organizational preparedness against cyber threats. The findings are relevant to a wide audience, including academics, organizations, policymakers, and technology developers. Scholars gain deeper insights, organizations receive actionable recommendations, policymakers gain valuable input for shaping policies, and technology developers benefit from practical implications for security implementation.

Keywords: Cybersecurity, Readiness, Dynamic Capabilities, Organizational Cybersecurity, Information Security Management

Introduction

In today's interconnected world, organizations face relentless sophisticated cyberattacks. Mandiant FireEye, (2023) reports that industries such as business & professional services, financial, high tech, and healthcare are consistently hardest hit. Since 2019, there's been a surge in malware and ransomware incidents, facilitated by readily available attack kits online. Cybercriminals refine tactics, leveraging rapid technological advancements, including machine learning-based methods (Mozo et al., 2022). Securing networks globally has become

increasingly complex. A successful attack can lead to severe consequences like lost revenue, customer attrition, legal repercussions, and reputational damage (Berlilana et al., 2021; Phillips & Tanner, 2019; Tu et al., 2018). This escalating threat landscape underscores the critical need for proactive cybersecurity readiness.

Cybersecurity protects an organization's IT assets—systems, networks, and data—from unauthorized access, ensuring business continuity. A strong strategy goes beyond technology, involving people and processes (Clark et al. 2020). The Information Security Management System (ISMS) categorizes security elements into three pillars: people, processes, and technology, addressed at strategic, tactical, and operational levels (Al-Karaki et al., 2022). Balancing these elements is crucial; overemphasizing one aspect exposes vulnerabilities.

To effectively manage cyber threats, organizations must integrate cybersecurity into their overarching business processes and practices. This involves tightly linking business processes, practices, and technology to foster robust security capabilities and dynamic adaptability. Dynamic Capabilities (DC) theory emphasizes sensing, seizing, and reconfiguring resources amid changing environments (Teece et al., 1997). DC encompasses both inherent abilities and systematic processes (Eisenhardt & Martin, 2000; Teece et al., 1997). In cybersecurity, this means harmonizing organizational abilities with structured processes to maintain an adaptive posture. Developing DC is essential for organizational readiness against evolving cyber threats, empowering effective sensing, seizing, and response (Naseer et al., 2018; Pigola & Rezende da Costa, 2023).

Studies by Hasan et al., (2021), Berlilana et al., (2021) and Bahuguna, Bisht, & Pande, (2019) emphasize the significant impact of cybersecurity readiness on organizational performance. These studies highlight the intricate nature of cybersecurity readiness, advocating for a holistic approach. Understanding the factors influencing readiness informs strategic investments in cyber capabilities. However, there's a gap in applying DC theory, which emphasizes organizational agility. Our study addresses this gap by using DC theory to analyse and categorize previous literature. This approach aligns with DC theory's focus on organizational abilities, providing a valuable framework for understanding and classifying cybersecurity readiness factors across different stages. It enables a deeper exploration of how organizations can sustain a competitive edge amidst evolving cyber threats.

Motivated by the growing need for effective cybersecurity strategies, this study contributes to both academic literature and practical applications. It offers a novel application of DC theory to cybersecurity readiness, exploring how organizations can build and enhance their capabilities to detect, respond to, and mitigate cyber threats. The study's findings provide valuable insights for academics, organizations, and policymakers, offering a comprehensive framework to inform decision-making and guide improvements in cybersecurity practices.

To address the outlined knowledge limitations, the attributes of cybersecurity readiness in organizations should be examined through a comprehensive literature review. This study addresses the research question: What key factors influencing cybersecurity readiness in organizations are discussed in the literature from 2014 to 2023?

The study uses thematic analysis with Atlas.ti 23, covering literature from 2014 to 2023, to comprehensively address relevant factors. By applying DC theory to cybersecurity, it offers valuable insights for academics, aids organizations in strategy enhancement, and provides policymakers with essential information for effective policies.

Background

Cybersecurity readiness reflects an organization's preparedness, capability, and commitment to counter cyber threats (Makridis & Smeets, 2018). Akhta et al. (2021) emphasize the need for high preparedness due to evolving threats. Lack of preparedness hampers security measures (Hasan et al., 2021). Safitra et al., (2023) advocate for a dynamic security approach focusing on resilience, digital skills, threat analysis, response plans, integration, readiness, flexibility, and collaboration. Organizational factors like industry, risk profile, size, resources, and regulatory requirements shape security approaches.

Bahuguna, Bisht, & Pande, (2019) highlight initiatives enhancing readiness through technical measures, organizational strategies, legal frameworks, capacity-building, cooperation, and information sharing. Neri et al., (2023) underscore the importance of awareness, culture, and resilience in cybersecurity readiness. Georgiadou et al., (2020) differentiate readiness factors at organizational and individual levels, including infrastructure, operations, policies, and employee security attitudes. IT managers' experience, best practices, network awareness, and user education impact readiness (Chapman & Reithel, 2021). Human factors like ignorance, negligence, and susceptibility necessitate mitigation through education, training, robust infrastructure, policies, and security investment (Quader & Janeja, 2021). Rodbert, (2020) emphasizes the importance of role understanding, shared beliefs, workplace culture, management support, continuous assessment, adaptive efforts, recognition, and educational training to mitigate insider threats.

Frameworks and models aid in assessing cybersecurity readiness. Georgiadou et al. (2020) proposed the Cyber-Security Culture Framework, evaluating workforce security readiness and resilience. Nweke et al. (2022) emphasized the crucial role of the cybersecurity workforce in building capabilities. Dahiya et al. (2022) highlighted the necessity of Cyber-Security Risk Management (CSRM) plans while Lee (2021) stressed the significance of risk management in enhancing cybersecurity readiness. Moreover, Berlilana et al. (2021) demonstrated the positive impact of cybersecurity readiness on security performance. Kour et al. (2020) provided guidance on responding to cyber threats at different organizational levels, and Hasan et al. (2021) identified various factors influencing readiness, including IT infrastructure and regulatory compliance. Marican et al. (2023) emphasized the importance of evaluating an organization's maturity in handling cybersecurity. This study aims to comprehensively analyse organizational facets beyond individual components, offering a nuanced and integrated approach to mitigate cybersecurity threats.

Managing cybersecurity readiness faces challenges from evolving threats, complex attacks, and persistent defence gaps. Organizations respond with dynamic defence mechanisms like moving target defence and mimic defence (Zheng et al., 2022). However, challenges persist due to the sophistication of cybercriminal tools and the relentless proliferation of threats (Mozo et al., 2022). Navigating this landscape requires ongoing refinement of capabilities and

resources. The existing literature on cybersecurity management forms a robust foundation for examining factors influencing readiness through the lens of DC.

Dynamic Capabilities in Cybersecurity Readiness

Dynamic capabilities (DC), as defined by Teece et al., (1997), involve organizations effectively integrating internal and external competences to adapt and remain competitive. Eisenhardt & Martin, (2000) describe DC as processes enabling firms to create new resource configurations through acquisition, release, modification, integration, or recombination of resources. Teece, (2012) further categorizes DC into three core capabilities: sensing, seizing, and transforming, which help organizations identify opportunities, mobilize resources, and sustain their competitive edge. Applying the DC framework to cybersecurity readiness allows organizations to strengthen their ability to prepare for and respond to emerging cyber threats by developing the necessary processes and capabilities to utilize resources effectively in an ever-changing environment (Baskerville et al., 2014; Naseer et al., 2018). According to Talafidaryani, (2021) and Steininger et al., (2022), DC is not only a widely recognized theory in information systems research but also a foundational concept in contemporary organizational sciences.

Studies by Chatfield & Reddick, (2019), Maynard et al., (2018), Shankar & Mohammed, (2020), and Naseer et al., (2023) have applied the DC theory to cybersecurity topics, such as the impact of cybersecurity policy and IoT on smart government, leveraging business analytics for dynamic capabilities in cybersecurity risk management, and overcoming data breach fallout. Naseer et al., (2023) specifically investigated real-time analytics for incident response agility through microfoundations like situational awareness, threat intelligence, and continuous monitoring (sensing capabilities), dynamic risk assessment, threat hunting, and automated responses (seizing capabilities), and reconfiguration of incident response procedures, redesigning workflows, and improving maturity (transforming capabilities). Despite these insights, research on cybersecurity readiness through the lens of DC theory remains limited. Therefore, this study aims to explore the factors influencing organizational cybersecurity readiness from the DC perspective.

Methodology

The study employs thematic review analysis using Atlas.ti 23, a methodology introduced by (Zairul, 2021). This approach aligns with the thematic analysis procedure commonly applied in literature reviews, involving the systematic identification of patterns and the construction of themes (Clarke & Braun, 2013). Atlas.ti 23 facilitates organizing and analysing qualitative data, establishing coding frameworks, annotations, and trend identification, ensuring consistency and rigor.

The literature search utilized Web of Science (WoS) and Scopus, renowned for comprehensive data coverage (Chadegani et al., 2013). WoS is a bibliographic pioneer, widely used for journal selection and research evaluation. Scopus considered superior in some aspects, offers reliable academic data. These databases were selected for their established reputation. The selection criteria included: 1) publication between 2014 and 2023; 2) articles containing at least one of the specified keywords in the title, abstract or keywords, such as “cybersecurity,” “information security,” “readiness,” “preparedness,” “mitigation,” “organization,” or “success factor.” The study focused solely on primary research, excluding review articles,

conference proceedings, book chapters, and non-English papers to align with its objectives. The initial search identified 285 articles (115 Scopus, 170 WoS).

Table I
Search strings from Scopus and WoS

SCOPUS	TITLE-ABS-KEY ("**cybersecurity**" OR "**cyber security**" OR "**information security**" AND "**readiness**" OR "**preparedness**" OR "**success factors**" AND "**organisations**" OR "**organizations**" OR "**firms**") AND PUBYEAR > **2013** AND PUBYEAR < **2024** AND (LIMIT-TO (DOCTYPE, "**ar**")) AND (LIMIT-TO (LANGUAGE, "**English**")) AND (LIMIT-TO(PUBSTAGE, "**final**"))	115 articles
WoS	**cybersecurity readiness organizations (Topic) or cyber security preparedness firm (Topic) or information security mitigation organization (Topic) or cybersecurity success factor (Topic) and Article (Document Types) and English (Languages) and 2023 or 2022 or 2021 or 2020 or 2019 or 2018 or 2017 or 2016 or 2015 or 2014 (Publication Years)**	170 articles

Data processing in Mendeley involved removing duplicates, updating author names, and verifying metadata, reducing the articles to 146. These were exported to Atlas.ti 23 for in-depth analysis of cybersecurity readiness factors. Bibliometric data like titles, publication years, author information, country, source periodical, keywords, and subject areas were extracted. Thematic analysis was conducted through thorough literature reading, and researchers reviewed and identified emerging themes related to factors affecting cybersecurity readiness. The study's findings include numerical data and recurring themes, shedding light on factors influencing cybersecurity readiness in organizations.

Results

The findings provide a descriptive overview of research trends and geographical dispersion. The subsequent section delves into a detailed exploration of the factors influencing cybersecurity readiness.

Descriptive Findings

Publication trends for organizational cybersecurity readiness were analysed based on year and geographic distribution. Fig. 1 shows the increasing number of articles from 2014 to 2023, with a significant rise between 2020 and 2021 (from 16 to 24 articles). Of the 146 studies, 76 used qualitative methodologies, 54 quantitative approaches, and 16 mixed methods.

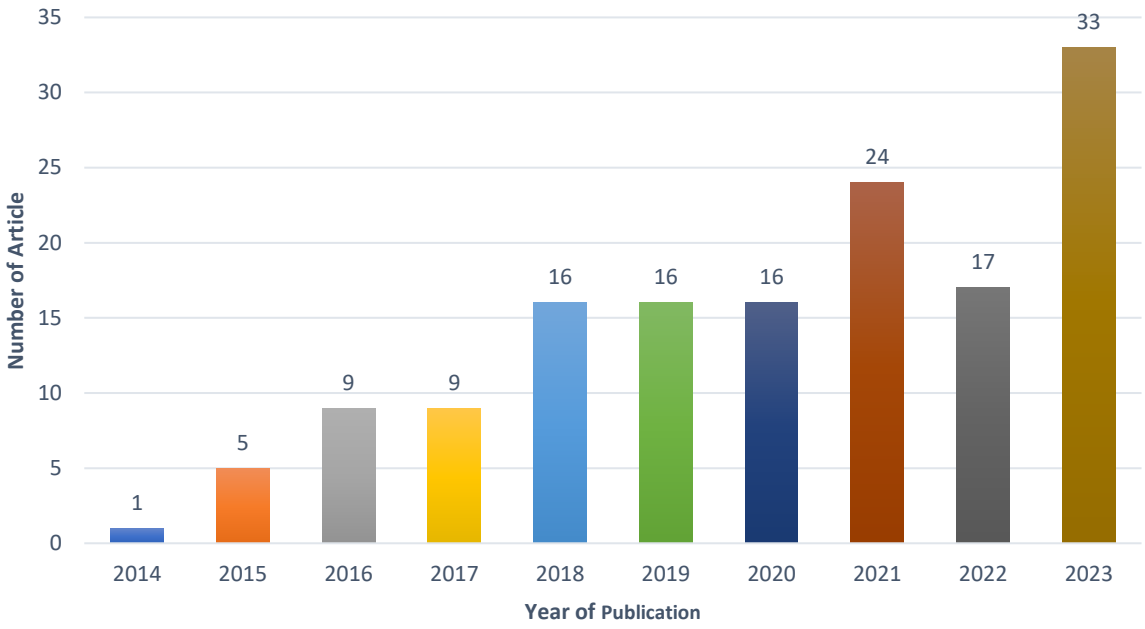

Figure I: Articles reviewed by year of publication
(Source(s): Author's own creation)

Regarding geographic distribution, the study prioritized the research focus location over author affiliation. When not explicitly stated, the first author's affiliation was used. The findings show global interest in organizational cybersecurity readiness research, with contributions from 43 countries (Figure 2). The United States led with 28 articles, followed by Malaysia (14) and the United Kingdom (12).

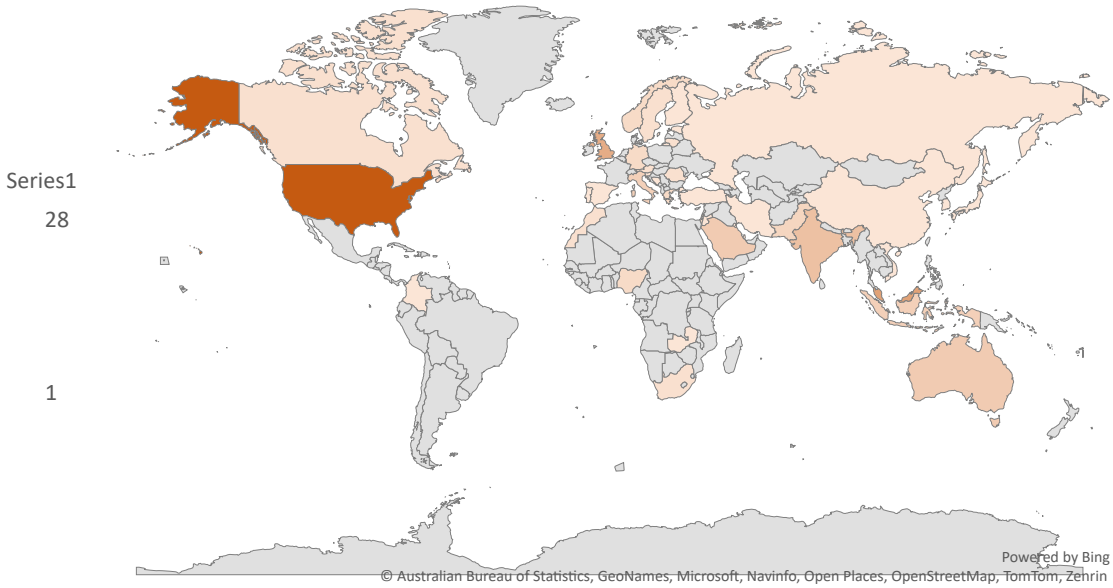

Figure II: Geographical Dispersion of Publications
(Source(s): Author's own creation)

A word cloud analysis of the 146 documents highlighted prominent terms, with 'security' (14,705 occurrences), 'information' (10,131), 'cyber' (6,990), and 'cyber security' (5,491) being

the most frequent. The analysis identified key themes and trends around factors affecting cybersecurity readiness, as shown in Fig. 3.

Figure III: Word Cloud Generated from the reviewed articles.
(Source(s): Author's own creation)

Cybersecurity Readiness Factors

Using DC as a theoretical lens, the study identified factors that impact cybersecurity readiness, categorizing them based on sensing, seizing, and transforming capabilities. The details of these factors are provided below.

Sensing Capabilities in Cybersecurity Readiness

Based on the review, the study identified that factors contributing to the development of sensing capabilities include situation awareness (Neri et al., 2024), threat intelligence (Brilingaitė et al., 2022), active surveillance (Kebande et al., 2021), technological adaptation (Zammani et al., 2019), and regulatory adaptation (Berlilana et al., 2021).

Table II
Factors Under Sensing Capabilities for Cybersecurity Readiness

Factor	Description	Sources
Situational Awareness	Situational awareness is crucial for cyber-attack readiness, relying on an understanding of the threat landscape, security trends, and vulnerabilities. It enables early detection, rapid response, and informed defensive decisions. Continuous updates from reliable data sources ensure agility against evolving threats.	(Chapman & Reithel, 2021; Falowo et al., 2022; Naseer et al., 2023; Neri et al., 2023)
Threat Intelligence	Threat intelligence provides insights into adversaries' intentions, capabilities, and opportunities, improving continuous threat detection. Integrating it with risk-based approaches and enterprise architecture strengthens cyber defences. Enhancing threat intelligence involves threat hunting and leveraging expert knowledge from actionable sources. Effective information sharing is crucial for collaboration and performance.	(Al-Kumaim & Alshamsi, 2023; Brilingaitė et al., 2022; Falowo et al., 2022; Hidayat & Wang, 2023; Phillips & Tanner, 2019; Randall & Allen, 2021; Serketzis et al., 2019; Zrahia, 2018)
Active Surveillance	Continuous network monitoring strengthens cybersecurity by enabling rapid detection and response to anomalies. Security Operations Centres (SOCs) support this through real-time monitoring, behaviour analysis, and sensor-based threat detection. Analytics and machine learning review logs for suspicious activities, while traffic analysers, sensors, and regular scans enhance attack detection and reduce risks.	(Buchler et al., 2018; Chapman & Reithel, 2021; Falowo et al., 2022; Joyce et al., 2021; Kebande et al., 2021; Larkin et al., 2014; Mehmood et al., 2023; Menachem et al., 2019; Naseer et al., 2021, 2023)
Technological Adaptation	Technological adaptation involves identifying and investing in security technologies, including the integration of advanced approaches such as AI and machine learning (ML). These technologies enhance threat detection, vulnerability identification, task automation, and the recognition of malicious network traffic patterns.	(Badi & Nasaj, 2023; Chindrus & Caruntu, 2023; Mehmood et al., 2023; Mishra et al., 2021; Mozo et al., 2022; Naseer et al., 2021; Quader & Janeja, 2021; Repetto et al., 2021; Safitra et al., 2023; Zammani et al., 2019)
Regulatory Adaptation	Regulatory adaptation involves complying with cybersecurity regulations and standards, enhancing an organization's readiness and ability to anticipate legal changes. Frameworks like ISO/IEC 27000, COBIT, ITIL, along with sector-specific requirements provide guidance, while international conventions such as the Budapest Convention support global cybercrime cooperation. Regular audits ensure adherence, strengthening cybersecurity practices.	(Al-Karaki et al., 2022; Alam & Ibrahim, 2021; AlMeraj et al., 2023; Berlilana et al., 2021; Ibrahim & Ali, 2018; Ifeanyi-Ajufo, 2023; Phillips & Tanner, 2019; Saban et al., 2021; Safitra et al., 2023; Tsen et al., 2022; Zhen et al., 2021)

Seizing Capabilities in Cybersecurity Readiness

Seizing capabilities are bolstered by dynamic risk management (Nicho, 2018), active cyber defence (Yeoh et al., 2023), resilience planning , data protection (Georgiadou et al., 2021), continuous training (Carlton et al., 2019), adaptive incident handling (Naseer et al., 2023), and access management (Ismail & Yusof, 2018).

Table III
Factors Under Seizing Capabilities for Cybersecurity Readiness

Factor	Description	Sources
Dynamic Risk Management	Dynamic risk management ensures agile responses to evolving cyber threats by continuously identifying, monitoring, and assessing real-time risks. It combines technical and procedural measures to mitigate both technological and human-related threats, protecting assets, enhancing agility, and ensuring continuity, including in interconnected supply chains. Cyber insurance acts as a proactive financial risk mitigation tool, covering recovery and business interruption costs. It incentivizes self-protection investments and enforces stringent cybersecurity controls among policyholders.	(AlMeraj et al., 2023; Bharathi, 2019; Biswas & Mukhopadhyay, 2018; Carlton et al., 2019; Creazza et al., 2022; Dzimiela & Jennex, 2023; Gonzalez-Granadillo et al., 2021; Lee et al., 2022; Menachem et al., 2019; Mott et al., 2023; Mukhopadhyay & Jain, 2023; Pandey et al., 2020; Silvestri et al., 2023; Skierka, 2023; Tarei et al., 2020; Taylor et al., 2016; Tu et al., 2018; Woszczynski & Green, 2017; Zammani et al., 2019)
Active Cyber Defence	Effective cybersecurity relies on essential active cyber defence technologies. These include antivirus, anti-malware, Endpoint Detection and Response (EDR), and Intrusion Detection Systems (IDS) for proactive threat detection and response. Mobile Device Management (MDM) facilitates device registration, visibility, and security. Regular security patching across network, application, operating system, and database levels is crucial for addressing vulnerabilities and bolstering endpoint security. Secure Software Development Lifecycle (SSDLC) models integrate security into the development process, ensuring secure applications in digital environments. Firewalls and Software Defined Networking (SDN) improve traffic visibility and anomaly detection, and integrating SDN with network segmentation, port control, and VPNs strengthens security, especially for remote work. VPNs and Two-Factor Authentication (2FA) counter threats like spam and phishing, securing connections in virtual organizations.	(Abdul Molok et al., 2018; Alam & Ibrahim, 2021; Colicchia et al., 2019; Falowo et al., 2022; Gandal et al., 2023; Georgiadou et al., 2022; Grubor et al., 2017; Hidayat & Wang, 2023; Humayun et al., 2023; Joyce et al., 2021; Larkin et al., 2014; Llanten-Lucio et al., 2022; Mjihil et al., 2016; Quader & Janeja, 2021; Sebastian & Glorin, 2021; Yauri & Abah, 2016; Yeoh et al., 2023)

Factor	Description	Sources
Resilience Planning	Resilience planning is crucial for cybersecurity, integrating strong policies, business continuity management (BCM), and the defence-in-depth concept. Security policies ensure compliance by outlining controls, responsibilities, and processes, with regular reviews to identify vulnerabilities. BCM ensures critical operations during disasters through recovery assessments, and data backups. Key elements include offsite backups, disaster recovery plans, and Business Impact Assessments. The defence-in-depth concept deploys controls across prevention, detection, response, and recovery stages, creating a robust framework against dynamic threats.	(Al-rimy et al., 2018; Alhogail et al., 2015; Almeida & Respício, 2018; Bello et al., 2017; bin Yeop et al., 2018; Chapman & Reithel, 2021; Creazza et al., 2022; Farshadkhah et al., 2021; Majid et al., 2021; Menachem et al., 2019; Miloslavskaya & Tolstaya, 2022; Mohamad Noorman Masrek et al., 2021; Neri et al., 2023; Phillips & Tanner, 2019; Quader & Janeja, 2021; Saban et al., 2021)
Data Protection	Data protection is vital for cybersecurity, ensuring confidentiality, integrity, and availability. Cyberattacks highlight the need for data loss prevention (DLP) measures like encryption, coding, and backups. Protecting proprietary information involves access restrictions, contractual agreements, breach penalties, and fostering ethical responsibility to deter unauthorized disclosure.	(Al-rimy et al., 2018; Colicchia et al., 2019; Georgiadou et al., 2021, 2022; Larkin et al., 2014; Majid et al., 2021; S, 2019; Tan et al., 2016; Tu et al., 2018; Yeoh et al., 2023)
Continuous Training and Skill Development	Continuous training in awareness, competency, and security education is key to cybersecurity readiness. Ongoing programs foster a security-conscious culture, but training should go beyond awareness to focus on building hands-on incident response skills. It should also be tailored to individual roles, not just IT specialists. Talent scouting is equally important for acquiring and retaining experts in hardware, software, and incident response.	(Alam & Ibrahim, 2021; Ani et al., 2019; Bartnes Line et al., 2016; Bello et al., 2017; Buchler et al., 2018; Carlton et al., 2019; Dzimiela & Jennex, 2023; Falowo et al., 2022; Mayer et al., 2017; Wong et al., 2019; Yeoh et al., 2023; Zammani et al., 2019)
Adaptive Incident Handling	Adaptive incident handling is essential for cybersecurity readiness, involving response plans, drills, forensics, and communication. Integrated with business continuity, these plans focus on swift action through automation and real-time monitoring, with clear roles and collaboration improving management. Regular	(Bahuguna, Bisht, Pande, et al., 2019; Brilingaitė et al., 2022; Buchler et al., 2018; Chindrus & Caruntu, 2023; Elyas et al., 2015; Falowo et al., 2022;

Factor	Description	Sources
	drills, like simulations and tabletop exercises, assess the plan's effectiveness and enhance teamwork. Learning from past incidents reinforces their value. Digital forensics supports real-time analysis, attacker identification, and prevention. Transparent communication reduces risks, prepares users, and builds public trust, while information-sharing platforms improve team coordination during incidents.	Grubor et al., 2017; Majid et al., 2021; Mozo et al., 2022; Naseer et al., 2021; Naseer et al., 2023; Phillips & Tanner, 2019; Skierka, 2023; Woszczynski & Green, 2017; Yeoh et al., 2023)
Access Management	Access management is key to cybersecurity, involving identity management, access control, and personnel screening to block unauthorized access. Essential measures include network policies, role segregation, wireless controls, multifactor authentication, and periodic access reviews, especially for remote work. For virtual organizations, it secures cloud access, enforces adaptive policies, manages privileged access, and governs sensitive data. Physical security is also crucial where regulating access to critical facilities like data centres, alongside personnel screening and background checks, helps reduce human-related risks.	(Al-rimy et al., 2018; Bahuguna, Bisht, Pande, et al., 2019; Chinyemba & Phiri, 2018; Colicchia et al., 2019; Creazza et al., 2022; Diesch et al., 2020; Georgiadou et al., 2020, 2021, 2022; Hidayat & Wang, 2023; Joyce et al., 2021; Kebande et al., 2021; Pandey et al., 2020; S, 2019; Sebastian & Glorin, 2021)

Transforming Capabilities for Cybersecurity Readiness

Transforming capabilities enable organizations to adapt and excel in the cybersecurity landscape. Factors such as strategic alignment (Tu et al., 2018), collaborative effort (Creazza et al., 2022), policy agility (Atkins & Lawson, 2021), security governance (Nicho, 2018), and security culture (Georgiadou et al., 2022) drive this transformation.

Table IV
Factors Under Transforming Capabilities for Cybersecurity Readiness

Factor	Description	Sources
Strategic Alignment	Strategic alignment integrates cybersecurity with organizational goals, securing top management support, and raising risk awareness. It ensures governance aligns with value delivery, risk management, and performance, resolving conflicts, boosting visibility, and aligning security with business strategies.	(Bernik & Prislan, 2016; Mayer et al., 2017; Nicho, 2018; Tu et al., 2018)
Collaborative Effort	Top management commitment and collaboration drive transformative cybersecurity capabilities by shaping a strong security culture and securing buy-in across all levels. Leadership fosters team dynamics and shared responsibility for cyber policies. Operational cooperation through information sharing and best practices strengthens defences. Establishing communication channels and collaborating with external parties enhances resilience. Suppliers, vendors, and partners are vital to the cybersecurity ecosystem, with collaboration strengthened through agreements, IT integration, and shared threat intelligence.	(Al-Kumaim & Alshamsi, 2023; Ani et al., 2019; Atkins & Lawson, 2021; Berlilana et al., 2021; Buchler et al., 2018; Chatterjee, 2019; Colicchia et al., 2019; Mayer et al., 2017; Mott et al., 2023; Safitra et al., 2023; Zammani et al., 2021; Zhen et al., 2021)
Policy Agility	Agile policies are crucial for adapting to evolving cyber threats and fostering resilience. Organizations enhance their security posture through regular reviews and updates using the Plan-Do-Check-Act cycle. Technology-neutral policies address dynamic challenges and adapt to advancements in cybersecurity risk management.	(Atkins & Lawson, 2021; Bernik & Prislan, 2016; Carlton et al., 2019; Miloslavskaya & Tolstaya, 2022; Safitra et al., 2023)
Security Governance	Security governance is crucial for cyber readiness, aligning processes with business strategies amid rising threats. Organizations use frameworks and standards to guide direction, risk management, and performance measurement, ensuring leadership engagement and accountability. Adaptive governance emphasizes flexibility and rapid decision-making. Globally, cyber governance is a policy priority, promoting security and stability through appropriate policies and cooperation.	(Almeida & Respício, 2018; Creazza et al., 2022; Gonzalez-Granadillo et al., 2021; Ifeanyi-Ajufo, 2023; Kiesling et al., 2016; Nicho, 2018; Skierka, 2023; Tarei et al., 2020; Tariq et al., 2020, 2017)
Security Culture	Cultivating a strong security culture is essential for cyber resilience. Leadership plays a key role as employees often follow cultural norms over formal policies. A positive security culture enhances preparedness, especially in managing errors, while mistrust hinders compliance. It involves collective awareness and shared responsibility, embedding cybersecurity into organizational norms. Incentives and penalties drive security culture. Recognition and rewards foster compliance, while disciplinary actions address insider threats. Legal penalties ensure regulatory compliance. Tailoring strategies to human behaviour, especially across diverse employee groups, enhances cybersecurity readiness.	(Alhogail et al., 2015; Bansal et al., 2023; Georgiadou et al., 2020, 2022; Hengstler et al., 2023; Ismail & Yusof, 2018; Mayer et al., 2017; Mohamad Noorman Masrek et al., 2021; Padayachee, 2022; Renaud et al., 2023; Rodbert, 2020; Taylor et al., 2016; Tu et al., 2018; Yeo & Banfield, 2022)

Dynamic Leadership

Dynamic cyber leadership, spearheaded by top management and a Chief Information Security Officer (CISO), is crucial for organizational resilience (Colicchia et al., 2019; Hidayat & Wang, 2023). The CISO sets goals, aligns strategies with business objectives, and oversees cyber activities (Repetto et al., 2021; Wong et al., 2019). Top management shapes compliance and fosters a high-performance security culture characterized by commitment, preparedness, and discipline (Chatterjee, 2019; Ismail & Yusof, 2018; Rodbert, 2020). Their active involvement correlates with engagement in proactive cyber measures, emphasizing leadership commitment, effective communication, and incentives to nurture a secure culture (Badi & Nasaj, 2023; Ibrahim & Ali, 2018).

Resource Allocation

Resource allocation in cybersecurity, covering funding, personnel, and technology, is crucial for achieving objectives like awareness, business continuity, and incident response (Bernik & Prislan, 2016; Falowo et al., 2022). Adequate funding secures devices and sustains cybersecurity measures (AlMeraj et al., 2023; Taylor et al., 2016). Investments require rigorous cost-benefit analyses, necessitating strong justifications for budget allocations (Chronopoulos et al., 2018; Miloslavskaya & Tolstaya, 2022). Cybersecurity disclosures impact investor perceptions, demanding increased investment in awareness and technology adoption (Cheng et al., 2022; Gandal et al., 2023; Quader & Janeja, 2021). Resource allocation should also prioritize development of skilled human resources (Alam & Ibrahim, 2021; Diesch et al., 2020).

Framework for Organizational Cybersecurity Readiness

The study's findings are synthesized into a comprehensive framework, presented in Fig. 5, which offers a valuable tool for understanding and enhancing organizational cybersecurity readiness.

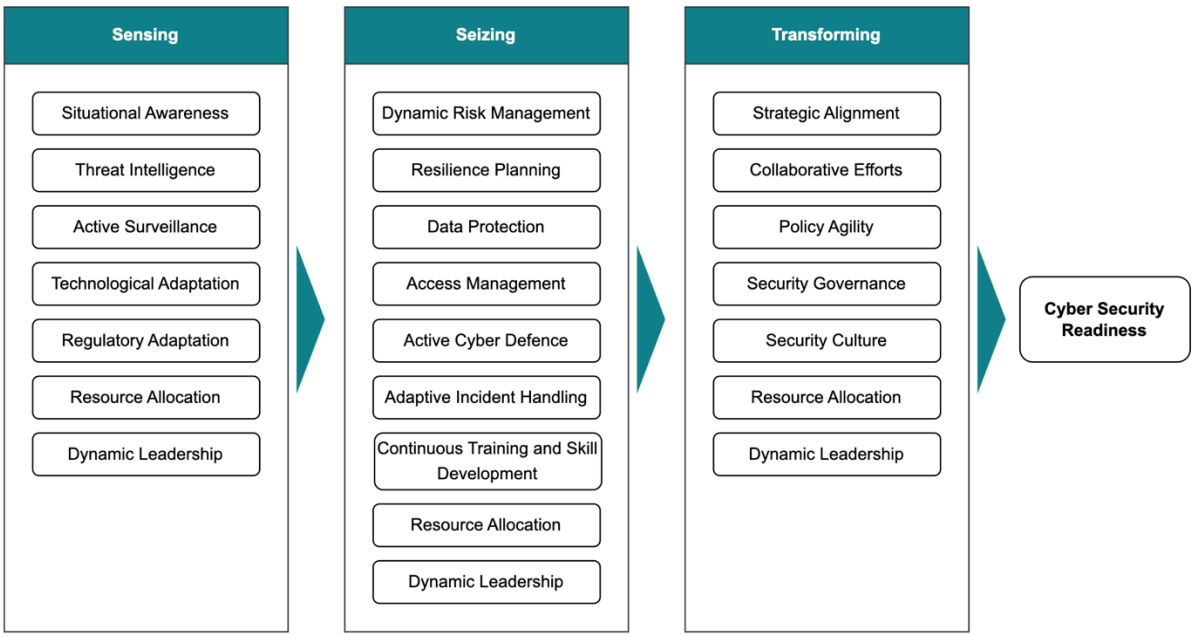

Figure IV: Building dynamic capabilities for cybersecurity readiness: a conceptual framework.

Discussion

The study employed a thematic review with Atlas.ti 23 software and a dynamic capabilities lens to analyze literature from 2014 to 2023, identifying factors shaping organizational cybersecurity readiness. The findings reveal a global increase in interest, reflecting cybersecurity's growing importance amid rising threats and shifting organizational priorities. These factors are categorized into sensing, seizing, and transforming capabilities, providing insights for addressing cybersecurity threats effectively.

Sensing capabilities, such as situational awareness, threat intelligence, and adaptive surveillance, are crucial for detecting and interpreting changes in the cybersecurity landscape. This aligns with research emphasizing their role in incident response frameworks (Naseer et al., 2023). Adapting to technological and regulatory shifts (Nylén & Holmström, 2015; Teece, 2009), highlights the importance of environmental monitoring (Sambamurthy et al., 2003) and agile responsiveness (Sher & Lee, 2004). Establishing comprehensive threat intelligence programs with dedicated teams enables swift adjustments to cybersecurity practices, proactively addressing vulnerabilities.

Seizing capabilities enable proactive threat responses, encompassing dynamic risk management, resilience planning, data protection, continuous training and skill development, adaptive incident handling, active cyber defence, and access management. Unlike Naseer et al., (2023), this study takes a comprehensive approach, integrating diverse elements contributing to proactive threat response. Technological solutions enhance cybersecurity posture (Neirotti & Raguseo, 2017; Pavlou & El Sawy, 2006) while resilience planning fosters innovative policies and procedures (Leidner et al., 2011). Human resources play a central role, emphasizing the need for awareness, competency, and skills to combat cyber threats (Cooper & Molla, 2017; Teece, 2012).

Transforming capabilities involve strategic integration, collaboration, policy agility, security governance, and fostering a strong security culture. These findings align with research on adaptability, flexibility, innovation, and information sharing amid evolving threats and technologies (Naseer et al., 2023). Aligning security efforts with organizational goals and maintaining agility to adapt to changes are crucial (Baker et al., 2011; Trinh-Phuong et al., 2012). Governance guides resource allocation and strategic direction (Busquets, 2015; Gregory et al., 2015), and a security-conscious culture is essential (Akter et al., 2021; Sousa-Zomer et al., 2020). Incentives and collaboration with stakeholders including partners, suppliers, and competitors are pivotal for comprehensive cybersecurity management (Bridoux et al., 2017; Côrte-Real et al., 2017; Köhler et al., 2022; Wójcik et al., 2022).

The study emphasizes the critical role of resource allocation and dynamic leadership in enhancing cybersecurity readiness. These factors, while not explicitly part of the sensing, seizing, and transforming framework, are vital to dynamic capabilities (Augier & Teece, 2009; Helfat & Peteraf, 2015; Teece, 2007). Financial capital and human resources are particularly crucial for creating and sustaining competitive advantage in cybersecurity readiness (Clark & Barney, 2007). Key factors essential for enhancing organizational cybersecurity readiness align with the dynamic capabilities framework proposed by Eisenhardt & Martin, (2000) and Teece et al., (1997). These factors also correspond with core elements in prominent cybersecurity standards like NIST, ISO/IEC 27002, and COBIT (Sulistyowati et al., 2020). However, achieving cybersecurity readiness is an ongoing process, requiring perpetual vigilance and adaptability to address the ever-changing cyber threat landscape.

Contributions and Limitation

This study contributes significantly to theory by applying DC theory to cybersecurity, enhancing our understanding of organizational adaptation to evolving threats. It presents a framework of multiple factors across sensing, seizing, and transforming capabilities, offering practical guidance and serving as a model for future research. Bridging literature gaps, it provides actionable insights and lays the groundwork for further exploration. Relevant to policymakers, practitioners, and academics, it offers insights into critical resources and processes for effective cybersecurity. Policymakers can use the findings to inform regulations, while organizations can strategically allocate resources to prevent data breaches and minimize financial losses, promoting cybersecurity resilience in our digitized world.

However, the study has limitations. It only included articles from Scopus and Web of Science databases, potentially overlooking relevant studies outside these platforms. The framework for organizational cybersecurity readiness, rooted in DC theory, enhances security practices, but future research should bolster its validity and practical applicability through comprehensive assessments using both quantitative and qualitative approaches. Quantitative research, such as surveys and statistical analyses, can offer broad insights from cybersecurity professionals and organizational leaders, revealing trends and areas for improvement within the framework. The study indicates a predominance of qualitative studies, possibly due to the absence of standardized measurement scales and challenges in scale development, emphasizing the need for more quantitative research. Qualitative research, employing in-depth interviews with cybersecurity experts, provides nuanced insights into the framework's application, strengths, weaknesses, and practical considerations. A mixed-methods approach will offer a holistic view, strengthening the framework's validity across diverse organizational

contexts. Despite these constraints, this paper significantly contributes to understanding factors influencing organizational cybersecurity readiness, laying the groundwork for future investigations.

References

Abdul Molok, N. N., Ahmad, A., & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. *International Journal of Information Management*, *43*(September), 351–356. https://doi.org/10.1016/j.ijinfomgt.2018.08.013

Akhta, S., Sheorey, P. A., Bhattacharya, S., & Ajith, K. V. V. (2021). Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *T*, *12*(1), 82–97. https://doi.org/10.4018/IJBIR.20210101.oa5

Akter, S., Wamba, S. F., Mariani, M., & Hani, U. (2021). How to Build an AI Climate-Driven Service Analytics Capability for Innovation and Performance in Industrial Markets? *Industrial Marketing Management*, *97*(January), 258–273. https://doi.org/10.1016/j.indmarman.2021.07.014

Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2022). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences*, *34*(6), 3079–3095. https://doi.org/10.1016/j.jksuci.2020.09.011

Al-Kumaim, N. H., & Alshamsi, S. K. (2023). Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership. *APPLIED SCIENCES-BASEL*, *13*(10). https://doi.org/10.3390/app13105839 WE - Science Citation Index Expanded (SCI-EXPANDED)

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166. https://doi.org/10.1016/j.cose.2018.01.001

Alam, R. G., & Ibrahim, H. (2021). Cybersecurity implementation success factors in smart city. *Journal of Theoretical and Applied Information Technology*, *99*(13), 3353–3364. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85110682680&partnerID=40&md5=cbb0d7a9af0949ff6a4208498c751471

Alhogail, A., Mirza, A., & Bakry, S. H. S. H. S. H. (2015). A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology*, *78*(2), 201–211.

Almeida, L., & Respício, A. (2018). Decision support for selecting information security controls. *Journal of Decision Systems*, *27*(sup1), 173–180. https://doi.org/10.1080/12460125.2018.1468177

AlMeraj, Z., Alenezi, A. K., & Manuel, P. D. (2023). An empirical investigation into organisation cyber security readiness from the IT employee and manager perspectives. *Electronic Government*, *19*(5), 539–559. https://doi.org/10.1504/EG.2023.133092

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Atkins, S., & Lawson, C. (2021). An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure. *Public Administration Review*, *81*(5), 847–861. https://doi.org/10.1111/puar.13322

Augier, M., & Teece, D. J. (2009). Dynamic capabilities and the role of managers in business

strategy and economic performance. *Organization Science*, *20*(2), 410–421. https://doi.org/10.1287/orsc.1090.0424

Badi, S., & Nasaj, M. (2023). Cybersecurity effectiveness in UK construction firms: an extended McKinsey 7S model approach. *Engineering, Construction and Architectural Management*. https://doi.org/10.1108/ECAM-12-2022-1131

Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. *Information Security Journal*, *28*(6), 164–177. https://doi.org/10.1080/19393555.2019.1689318

Bahuguna, A., Bisht, R. K., Pande, J., Bahuguna*, A., Bisht, R. K., & Pande, J. (2019). Don't Wanna Cry: A Cyber Crisis Table Top Exercise for Assessing the Preparedness against Eminent Threats. *International Journal of Engineering and Advanced Technology*, *9*(1), 3705–3710. https://doi.org/10.35940/ijeat.A9893.109119

Baker, J., Jones, D. R., Cao, Q., & Song, J. (2011). Conceptualizing the dynamic strategic alignment competency. *Journal of the Association for Information Systems*, *12*(4), 299–322. https://doi.org/10.17705/1jais.00265

Bansal, G., Thatcher, J., & Schuetz, S. W. (2023). Where authorities fail and experts excel: Influencing internet users' compliance intentions. *Computers & Security*, *128*, 103164. https://doi.org/10.1016/j.cose.2023.103164

Bartnes Line, M., Anne Tøndel, I., & Jaatun, M. G. M. G. (2016). Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter? Information security incident management in large and small industrial control organizations. *International Journal of Critical Infrastructure Protection*, *12*, 12–26. https://doi.org/10.1016/j.ijcip.2015.12.003

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management*, *51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Bello, A. G., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information & Computer Security*, *25*(4), 475–492. https://doi.org/10.1108/ICS-03-2016-0025

Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLoS ONE*, *11*(9), 1–33. https://doi.org/10.1371/journal.pone.0163050

Berrada, H., Boutahar, J., & Houssaïni, S. E. G. El. (2021). Simplified IT Risk Management Maturity Audit System based on "COBIT 5 for Risk." *International Journal of Advanced Computer Science and Applications*, *12*(8), 641–652. https://doi.org/10.14569/IJACSA.2021.0120875

Bharathi, S. V. (2019). Forewarned is forearmed: Assessment of IoT information security risks using analytic hierarchy process. *Benchmarking: An International Journal*, *26*(8), 2443–2467. https://doi.org/10.1108/BIJ-08-2018-0264

bin Yeop, Y. H., Othman, Z. A., Abdullah, S. N. H. S., Mokhtar, U. A., & Fauzi, W. F. P. (2018). BYOD implementation factors in schools: A case study in Malaysia. *International Journal of Advanced Computer Science and Applications*, *9*(12), 311–317. https://doi.org/10.14569/IJACSA.2018.091245

Biswas, B., & Mukhopadhyay, A. (2018). G-RAM framework for software risk assessment and mitigation strategies in organisations. *Journal of Enterprise Information Management*, *31*(2), 276–299. https://doi.org/10.1108/JEIM-05-2017-0069

Bridoux, F., Coeurderoy, R., & Durand, R. (2017). Heterogeneous social motives and

interactions: The three predictable paths of capability development. *Strategic Management Journal*, *38*(9), 1755–1773. https://doi.org/10.1002/smj.2605

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. *Journal of Cybersecurity*, *8*(1). https://doi.org/10.1093/cybsec/tyac001

Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P., Marusich, L., & Lightner, L. (2018). Cyber Teaming and Role Specialization in a Cyber Security Defense Competition. *Frontiers in Psychology*, *9*. https://doi.org/10.3389/fpsyg.2018.02133

Busquets, J. (2015). Discovery paths: Exploring emergence and IT evolutionary design in cross-border M and As. Analysing grupo Santander's acquisition of abbey (2004-2009). *European Journal of Information Systems*, *24*(2), 178–201. https://doi.org/10.1057/ejis.2014.38

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*, *27*(1), 101–121. https://doi.org/10.1108/ICS-11-2016-0088

Chadegani, A. A., Salehi, H., Yunus, M. M., Farhadi, H., Fooladi, M., Farhadi, M., & Ebrahim, N. A. (2013). A Comparison between Two Main Academic Literature Collections: Web of Science and Scopus Databases. *Asian Social Science*, *9*(5). https://doi.org/10.5539/ass.v9n5p18

Chapman, T. A., & Reithel, B. J. (2021). Perceptions of Cybersecurity Readiness among Workgroup IT Managers. *Journal of Computer Information Systems*, *61*(5), 438–449. https://doi.org/10.1080/08874417.2019.1703224

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, *36*(2), 346–357. https://doi.org/10.1016/j.giq.2018.09.007

Chatterjee, D. (2019). Should executives go to jail over cybersecurity breaches? *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 1–3. https://doi.org/10.1080/10919392.2019.1568713

Cheng, X., Hsu, C., & Wang, T. (David). (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. *Communications of the Association for Information Systems*, *50*(1), 481–485. https://doi.org/10.17705/1CAIS.05022

Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. *Information (Switzerland)*, *14*(11). https://doi.org/10.3390/info14110587

Chinyemba, M. K., & Phiri, J. (2018). An Investigation into Information Security Threats from Insiders and how to Mitigate them: A Case Study of Zambian Public Sector. *Journal of Computer Science*, *14*(10), 1389–1400. https://doi.org/10.3844/jcssp.2018.1389.1400

Chronopoulos, M., Panaousis, E., & Grossklags, J. (2018). An Options Approach to Cybersecurity Investment. *IEEE Access*, *6*(c), 12175–12186. https://doi.org/10.1109/ACCESS.2017.2773366

CÎRNU, C. E., ROTUNĂ, C. I., VEVERA, A. V., & BONCEA, R. (2018). Measures to Mitigate Cybersecurity Risks and Vulnerabilities in Service-Oriented Architecture. *Studies in Informatics and Control*, *27*(3), 359–368. https://doi.org/10.24846/v27i3y201811

Clark, D., & Barney, J. (2007). *Resource-Based Theory: Creating and Sustaining Competitive Advantage*. Oxford University Press.

Clark, M. A., Espinosa, J. A., & DeLone, W. H. (2020). Defending organizational assets: A

preliminary framework for cybersecurity success and knowledge alignment. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 4283–4292. https://doi.org/10.24251/hicss.2020.524

Clarke, V., & Braun, V. (2013). Teaching thematic analysis : Overcoming challenges and developing strategies for effective learning Associate Professor in Sexuality Studies Department of Psychology Faculty of Health and Life Sciences University of the West of England Coldharbour Lane Br. *University of the West of England*, *26*, 120–123.

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), 215–240. https://doi.org/10.1108/SCM-09-2017-0289

Cooper, V., & Molla, A. (2017). Information systems absorptive capacity for environmentally driven IS-enabled transformation. *Information Systems Journal*, *27*(4), 379–425. https://doi.org/10.1111/isj.12109

Côrte-Real, N., Oliveira, T., & Ruivo, P. (2017). Assessing business value of Big Data Analytics in European firms. *Journal of Business Research*, *70*, 379–390. https://doi.org/10.1016/j.jbusres.2016.08.011

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, *27*(1), 30–53. https://doi.org/10.1108/SCM-02-2020-0073

Dahiya, M., Nitin, N., & Dahiya, D. (2022). Intelligent Cyber Security Framework Based on SC-AJSO Feature Selection and HT-RLSTM Attack Detection. *Applied Sciences (Switzerland)*, *12*(13). https://doi.org/10.3390/app12136314

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. *IEEE ACCESS*, *11*, 125138–125158. https://doi.org/10.1109/ACCESS.2023.3327016

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers and Security*, *92*. https://doi.org/10.1016/j.cose.2020.101747

Dönmez, E., Kitapçı, N., Kitapçı, O., Yay, M., Aksu, P., Köksal, L., & Mumcu, G. (2020). Readiness for Health Information Technology is Associated to Information Security in Healthcare Institutions. *Acta Informatica Medica*, *28*(4), 265. https://doi.org/10.5455/aim.2020.28.265-271

Dzimiela, C., & Jennex, M. E. M. E. (2023). An Inside View of a Ransomware Attack Response and Recovery. *Journal of Information Systems Security*, *19*(2), 97–114.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*(10–11), 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11<1105::AID-SMJ133>3.0.CO;2-E

Elyas, M., Ahmad, A., Maynard, S. B. S. B. S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers and Security*, *52*, 70–89. https://doi.org/10.1016/j.cose.2015.04.003

Fainshmidt, S., & Frazier, M. L. (2017). What Facilitates Dynamic Capabilities? The Role of Organizational Climate for Trust. *Long Range Planning*, *50*(5), 550–566. https://doi.org/10.1016/j.lrp.2016.05.005

Fallon-Byrne, L., & Harney, B. (2017). Microfoundations of dynamic capabilities for innovation: a review and research agenda. *The Irish Journal of Management*, *36*(1), 21–

31. https://doi.org/10.1515/ijm-2017-0004

Falowo, O. I., Popoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. *IEEE Access*, *10*, 134038–134051. https://doi.org/10.1109/ACCESS.2022.3231847

Farshadkhah, S., Van Slyke, C., & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers & Security*, *100*, 102082. https://doi.org/10.1016/j.cose.2020.102082

Gandal, N., Moore, T., Riordan, M., & Barnir, N. (2023). Empirically evaluating the effect of security precautions on cyber incidents. *Computers & Security*, *133*, 103380. https://doi.org/10.1016/j.cose.2023.103380

Gbadeyan, A., Butakov, S., & Aghili, S. (2017). IT governance and risk mitigation approach for private cloud adoption: case study of provincial healthcare provider. *Annals of Telecommunications*, *72*(5–6), 347–357. https://doi.org/10.1007/s12243-017-0568-5

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9). https://doi.org/10.3390/s21093267

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35*(2), 486–505. https://doi.org/10.1057/s41284-021-00286-2

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., Nifakos, S., Xenakis, C., & Panaousis, E. (2021). Automated Cyber and Privacy Risk Management Toolkit. *Sensors*, *21*(16), 5493. https://doi.org/10.3390/s21165493

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm (CyFEr): Prioritized Gap Analysis. *IEEE Systems Journal*, *14*(2), 1897–1908. https://doi.org/10.1109/JSYST.2019.2913141

Gregory, R. W., Keil, M., Muntermann, J., & Mähring, M. (2015). Paradoxes and the nature of ambidexterity in IT transformation programs. *Information Systems Research*, *26*(1), 57–80. https://doi.org/10.1287/isre.2014.0554

Grubor, G., Barac, I., Simeunovic, N., & Ristic, N. (2017). Achieving business excellence by optimizing corporate forensic readiness. *Amfiteatru Economic*, *19*(44), 197–214. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85013036499&partnerID=40&md5=d38a9f38999b289402c9bfa4f25c9c41

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Helfat, C. E., & Peteraf, M. A. (2015). Managerial cognitive capabilities and the microfoundations of dynamic capabilities. *Strategic Management Journal*, *36*(6), 831–850. https://doi.org/10.1002/smj.2247

Hengstler, S., Kuehnel, S., Masuch, K., Nastjuk, I., & Trang, S. (2023). Should I Really do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior. *Computers & Security*, *133*, 103370. https://doi.org/10.1016/j.cose.2023.103370

Hidayat, V. K., & Wang, G. (2023). A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution. *Journal of System and Management Sciences*, *13*(5), 525–543. https://doi.org/10.33168/JSMS.2023.0534

Humayun, M., Niazi, M., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2023). Toward a readiness model for secure software coding. *Software - Practice and Experience*, *53*(4), 1013–1035. https://doi.org/10.1002/spe.3175

Ibrahim, N., & Ali, N. (2018). The role of organizational factors to the effectiveness of ISMS implementation in Malaysian Public Sector. *International Journal of Engineering and Technology(UAE)*, *7*(4), 544–550. https://doi.org/10.14419/ijet.v7i4.35.22907

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. *POLICY DESIGN AND PRACTICE*, *6*(2), 146–159. https://doi.org/10.1080/25741292.2023.2199960

Ismail, W. B. W., & Yusof, M. (2018). Mitigation Strategies for Unintentional Insider Threats on Information Leaks. *International Journal of Security and Its Applications*, *12*(1), 37–46. https://doi.org/10.14257/ijsia.2018.12.1.03

Iyengar, K., Sweeney, J. R., & Montealegre, R. (2015). Information technology use as a learning mechanism: The impact of it use on knowledge transfer effectiveness, absorptive capacity, and franchisee performance. *MIS Quarterly: Management Information Systems*, *39*(3), 615–641. https://doi.org/10.25300/MISQ/2015/39.3.05

Javaheri, D., Gorgin, S., Lee, J. A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *INFORMATION SCIENCES*, *626*, 315–338. https://doi.org/10.1016/j.ins.2023.01.067

Jesus, V., Bains, B., & Chang, V. (2023). Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence. *IEEE Transactions on Engineering Management*, *PP*, 1–20. https://doi.org/10.1109/TEM.2023.3279274

Joyce, C., Roman, F. L., Miller, B., Jeffries, J., & Miller, R. C. (2021). Emerging Cybersecurity Threats in Radiation Oncology. *Advances in Radiation Oncology*, *6*(6), 100796. https://doi.org/10.1016/j.adro.2021.100796

Karjalainen, M., Ojala, A.-L., Vatanen, M., & Lötjönen, J. (2023). Learn to Train Like You Fight. *International Journal of Adult Education and Technology*, *14*(1), 1–20. https://doi.org/10.4018/IJAET.322085

Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2021). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*, *13*(1), 5–17. https://doi.org/10.1007/s41870-020-00585-8

Kiesling, E., Ekelhart, A., Grill, B., Strauss, C., & Stummer, C. (2016). Selecting security control portfolios: a multi-objective simulation-optimization approach. *EURO Journal on Decision Processes*, *4*(1–2), 85–117. https://doi.org/10.1007/s40070-016-0055-7

Köhler, J., Sönnichsen, S. D., & Beske-Jansen, P. (2022). Towards a collaboration framework for circular economy: The role of dynamic capabilities and open innovation. *Business Strategy and the Environment*, *31*(6), 2700–2713. https://doi.org/10.1002/bse.3000

Kor, Y. Y., & Mahoney, J. T. (2005). How dynamics, management, and governance of resource deployments influence firm-level performance. *Strategic Management Journal*, *26*(5), 489–496. https://doi.org/10.1002/smj.459

Kour, R., Karim, R., & Thaduri, A. (2020). Cybersecurity for railways – A maturity model. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, *234*(10), 1129–1148. https://doi.org/10.1177/0954409719881849

Lado, A. A., & Wilson, M. C. (1994). Human Resource Systems and Sustained Competitive Advantage: A Competency-Based Perspective. *The Academy of Management Review*,

19(4), 699. https://doi.org/10.2307/258742

Larkin, R. D., Lopez Jr., J., Butts, J. W., & Grimaila, M. R. (2014). Evaluation of Security Solutions in the SCADA Environment. *DATA BASE FOR ADVANCES IN INFORMATION SYSTEMS*, *45*(1), 38–53. https://doi.org/10.1145/2591056.2591060

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Lee, J., de Guzman, M. C., Wang, J., Gupta, M., & Rao, H. R. (2022). Investigating perceptions about risk of data breaches in financial institutions: A routine activity-approach. *Computers & Security*, *121*, 102832. https://doi.org/10.1016/j.cose.2022.102832

Leidner, D. E., Lo, J., & Preston, D. (2011). An empirical investigation of the relationship of IS strategy with firm performance. *Journal of Strategic Information Systems*, *20*(4), 419–437. https://doi.org/10.1016/j.jsis.2011.09.001

Liu, H., Ke, W., Wei, K. K., & Hua, Z. (2013). The impact of IT capabilities on firm performance: The mediating roles of absorptive capacity and supply chain agility. *Decision Support Systems*, *54*(3), 1452–1462. https://doi.org/10.1016/j.dss.2012.12.016

Llanten-Lucio, Y.-I., Amador-Donado, S., & Marceles-Villalba, K. (2022). Validation of Cybersecurity Framework for Threat Mitigation. *Revista Facultad de Ingeniería*, *31*(62), e14840. https://doi.org/10.19053/01211129.v31.n62.2022.14840

Majid, M. A., Ariffin, K. A. Z., Abd Majid, M., Zainol Ariffin, K. A., Majid, M. A., Ariffin, K. A. Z., Abd Majid, M., & Zainol Ariffin, K. A. (2021). Model for successful development and implementation of Cyber Security Operations Centre (SOC). *PLoS ONE*, *16*(11 November), e0260157. https://doi.org/10.1371/journal.pone.0260157

Makridis, C. A., & Smeets, M. (2018). Determinants of cyber readiness. *SSRN Electronic Journal*, *4*(1), 72–89. https://doi.org/10.2139/ssrn.3216231

Mandiant FireEye. (2023). *M-Report 2023*.

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, *11*(August 2022), 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

Mayer, P., Gerber, N., McDermott, R., Volkamer, M., & Vogt, J. (2017). Productivity vs security: mitigating conflicting goals in organizations. *Information & Computer Security*, *25*(2), 137–151. https://doi.org/10.1108/ICS-03-2017-0014

Mehmood, M., Amin, R., Muslam, M. M. A., Xie, J., & Aldabbas, H. (2023). Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning. *IEEE ACCESS*, *11*, 46561–46576. https://doi.org/10.1109/ACCESS.2023.3273895 WE - Science Citation Index Expanded (SCI-EXPANDED)

Menachem, D., Sujata, J., & Roshan, P. (2019). Risk Mitigation Model for Data Loss: A Case Study Approach. *Journal of Advanced Research in Dynamical and Control Systems*, *11*(0009-SPECIAL ISSUE), 440–447. https://doi.org/10.5373/JARDCS/V11/20192590

Miloslavskaya, N., & Tolstaya, S. (2022). Information Security Management Maturity Models. *Procedia Computer Science*, *213*(C), 49–57. https://doi.org/10.1016/j.procs.2022.11.037

Mishra, S., Sharma, S. K., Alowaidi, M. A., Kumar Sharma, S., & A. Alowaidi, M. (2021). Multilayer self-defense system to protect enterprise cloud. *Computers, Materials and Continua*, *66*(1), 71–85. https://doi.org/10.32604/cmc.2020.012475

Mjihil, O., Kim, D. S., & Haqiq, A. (2016). Security Assessment Framework for Multi-tenant Cloud with Nested Virtualization. *JOURNAL OF INFORMATION ASSURANCE AND SECURITY*, *11*(5), 283–292.

Mohamad Noorman Masrek, Tri Soesantari, Asad Khan, & Aang Kisnu Dermawan. (2021).

Examining the Relationship between Information Security Effectiveness and Information Security Threats. *International Journal of Business and Society*, *21*(3), 1203–1214. https://doi.org/10.33736/ijbs.3335.2020

Mott, G., Turner, S., Nurse, J. R. C., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. *Computers & Security*, *128*(November 2022), 103162. https://doi.org/10.1016/j.cose.2023.103162

Mozo, A., Pastor, A., Karamchandani, A., de la Cal, L., Rivera, D., & Moreno, J. I. (2022). Integration of Machine Learning-Based Attack Detectors into Defensive Exercises of a 5G Cyber Range. *Applied Sciences*, *12*(20), 10349. https://doi.org/10.3390/app122010349

Mukhopadhyay, A., & Jain, S. (2023). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management*, *74*(January 2023), 102724. https://doi.org/10.1016/j.ijinfomgt.2023.102724

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, *59*(February), 102334. https://doi.org/10.1016/j.ijinfomgt.2021.102334

Naseer, H., Desouza, K., Maynard, S. B., & Ahmad, A. (2024). Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. *European Journal of Information Systems*, *33*(2), 200–220. https://doi.org/10.1080/0960085X.2023.2257168

Naseer, H., Maynard, S. B., Ahmad, A., & Shanks, G. (2018). Cybersecurity Risk Management Using Analytics : A Dynamic Capabilities Approach. *Thirty Ninth International Conference on Information Systems*, *2*, 1–9.

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*(June 2020), 113476. https://doi.org/10.1016/j.dss.2020.113476

Neirotti, P., & Raguseo, E. (2017). On the contingent value of IT-based capabilities for the competitive advantage of SMEs: Mechanisms and empirical evidence. *Information and Management*, *54*(2), 139–153. https://doi.org/10.1016/j.im.2016.05.004

Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information & Computer Security*, *32*(1), 38–52. https://doi.org/10.1108/ICS-05-2023-0084

Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ICS-07-2016-0061

Nweke, L. O., Bokolo, A. J., Mba, G., & Nwigwe, E. (2022). Investigating the effectiveness of a HyFlex cyber security training in a developing country: A case study. *Education and Information Technologies*, *27*(7), 10107–10133. https://doi.org/10.1007/s10639-022-11038-z

Nylén, D., & Holmström, J. (2015). Digital innovation strategy: A framework for diagnosing and improving digital product and service innovation. *Business Horizons*, *58*(1), 57–67. https://doi.org/10.1016/j.bushor.2014.09.001

Padayachee, K. (2022). Understanding the effects of situational crime prevention and personality factors on insider compliance. *Journal of Information Security and Applications*, *70*, 103338. https://doi.org/10.1016/j.jisa.2022.103338

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128. https://doi.org/10.1108/JGOSS-05-2019-0042

Pavlou, P. A., & El Sawy, O. A. (2006). From IT leveraging competence to competitive advantage in turbulent environments: The case of new product development. *Information Systems Research*, *17*(3), 198–227. https://doi.org/10.1287/isre.1060.0094

Pham, H. C., Brennan, L., Parker, L., Phan-Le, N. T., Ulhaq, I., Nkhoma, M. Z., & Nhat Nguyen, M. (2019). Enhancing cyber security behavior: an internal social marketing approach. *Information & Computer Security*, *28*(2), 133–159. https://doi.org/10.1108/ICS-01-2019-0023

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224–232. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85062890246&partnerID=40&md5=4167e2be8fcda1690ed7d78b907b5303

Pigola, A., & Rezende da Costa, P. (2023). Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats. *Communications of the Association for Information Systems*, *53*(1), 1099–1135. https://doi.org/10.17705/1CAIS.05347

Quader, F., & Janeja, V. P. (2021). Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies. *Journal of Cybersecurity and Privacy*, *1*(4), 638–659. https://doi.org/10.3390/jcp1040032

Randall, R. G., & Allen, S. (2021). Cybersecurity professionals information sharing sources and networks in the U.S. electrical power industry. *International Journal of Critical Infrastructure Protection*, *34*(June), 100454. https://doi.org/10.1016/j.ijcip.2021.100454

Renaud, K., Warkentin, M., Pogrebna, G., & van der Schyff, K. (2023). VISTA: An inclusive insider threat taxonomy, with mitigation strategies. *INFORMATION \& MANAGEMENT*, *61*(1), 103877. https://doi.org/10.1016/j.im.2023.103877

Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G., & Bolla, R. (2021). An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains. *Journal of Network and Systems Management*, *29*(4), 37. https://doi.org/10.1007/s10922-021-09607-7

Rindova, V. P. ., & Kotha, S. (2001). Continuous " Morphing ": Competing through Dynamic Capabilities , Form , and Function. *Academy of Management Journal*, *44*(6), 1263–1280.

Rodbert, M. (2020). Why organisational readiness is vital in the fight against insider threats. *Network Security*, *2020*(8), 7–9. https://doi.org/10.1016/S1353-4858(20)30092-1

Saban, K. A., Rau, S., & Wood, C. A. (2021). “SME executives’ perceptions and the information security preparedness model”. *Information and Computer Security*, *29*(2), 263–282. https://doi.org/10.1108/ICS-01-2020-0014

Saeed, K., Tariq, R., Khalil, W., Ahmed, S., Ali, M. T., Hassan, F., & Khattak, M. N. K. (2019). A Comprehensive Analysis of Cyber Security Attacks in Virtual Organizations with their Mitigation Plans. *JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES*, *14*(3), 454–468. https://doi.org/10.26782/jmcms.2019.06.00035

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability (Switzerland)*, *15*(18). https://doi.org/10.3390/su151813369

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *MIS Quarterly: Management Information Systems*, *27*(2), 237–264.

https://doi.org/10.2307/30036530

Samonas, S., Dhillon, G., & Almusharraf, A. (2020). Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management*, *50*(September 2018), 144–154. https://doi.org/10.1016/j.ijinfomgt.2019.04.011

Sebastian, G., & Glorin, S. (2021). A Descriptive Study on Cybersecurity Challenges of Working from Home during COVID-19 Pandemic and a Proposed 8 step WFH Cyber-attack Mitigation Plan. *Communications of the IBIMA*, *2021*, 1–7. https://doi.org/10.5171/2021.589235

Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D., & Pangalos, G. J. (2019). Actionable threat intelligence for digital forensics readiness. *Information and Computer Security*, *27*(2), 273–291. https://doi.org/10.1108/ICS-09-2018-0110

Shankar, N., & Mohammed, Z. (2020). Surviving Data Breaches: A Multiple Case Study Analysis. *Journal of Comparative International Management*, *23*(1), 35–54. https://doi.org/10.7202/1071508ar

Sher, P. J., & Lee, V. C. (2004). Information technology as a facilitator for enhancing dynamic capabilities through knowledge management. *Information and Management*, *41*(8), 933–945. https://doi.org/10.1016/j.im.2003.06.004

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing Informational Disadvantages to Improve Cyber Risk Management†. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *43*(2), 224–238. https://doi.org/10.1057/s41288-018-0078-3

Silvestri, S., Islam, S., Amelin, D., Weiler, G., Papastergiou, S., & Ciampi, M. (2023). Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. *International Journal of Information Security*, *23*(1), 31–50. https://doi.org/10.1007/s10207-023-00769-w

Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *GOVERNMENT INFORMATION QUARTERLY*, *40*(1). https://doi.org/10.1016/j.giq.2022.101781 WE - Social Science Citation Index (SSCI)

Sousa-Zomer, T. T., Neely, A., & Martinez, V. (2020). Digital transforming capability and performance: a microfoundational perspective. *International Journal of Operations & Production Management*, *40*(7/8), 1095–1128. https://doi.org/10.1108/IJOPM-06-2019-0444

Steininger, D. M., Mikalef, P., Pateli, A., & Ortiz-de-Guinea, A. (2022). Dynamic Capabilities in Information Systems Research: A Critical Review, Synthesis of Current Knowledge, and Recommendations for Future Research. *Journal of the Association for Information Systems*, *22*(2), 447–490. https://doi.org/10.17705/1jais.00736

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV : International Journal on Informatics Visualization*, *4*(4), 225. https://doi.org/10.30630/joiv.4.4.482

Talafidaryani, M. (2021). A text mining-based review of the literature on dynamic capabilities perspective in information systems research. *Management Research Review*, *44*(2), 236–267. https://doi.org/10.1108/MRR-03-2020-0139

Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and Knowledge Leakage in Supply Chain. *INFORMATION SYSTEMS FRONTIERS*, *18*(3), 621–638.

https://doi.org/10.1007/s10796-015-9553-6

Tarei, P. K., Thakkar, J. J., & Nag, B. (2020). Development of a decision support system for assessing the supply chain risk mitigation strategies: an application in Indian petroleum supply chain. *Journal of Manufacturing Technology Management*, *32*(2), 506–535. https://doi.org/10.1108/JMTM-02-2020-0035

Tariq, M. I., Ahmed, S., Memon, N. A., Tayyaba, S., Ashraf, M. W., Nazir, M., Hussain, A., Balas, V. E., & Balas, M. M. (2020). Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks. *Sensors*, *20*(5), 1310. https://doi.org/10.3390/s20051310

Tariq, M. I., Tayyaba, S., Hashmi, M. U., Ashraf, M. W., & Mian, N. A. (2017). Agent Based Information Security Threat Management Framework for Hybrid Cloud Computing. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY*, *17*(12), 57–66.

Taylor, R. G. R. G., Brice, J., & Robinson, S. L. S. L. (2016). Perception deception: security risks created by optimistic perceptions. *Journal of Systems and Information Technology*, *18*(1), 2–17. https://doi.org/10.1108/JSIT-07-2015-0062

Teece, D. J. (2007). Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350. https://doi.org/10.1002/smj.640

Teece, D. J. (2009). *Dynamic Capabilities and Strategic Management: Organizing for Innovation and Growth*. Oxford University Press.

Teece, D. J. (2012). Dynamic Capabilities: Routines versus Entrepreneurial Action. *Journal of Management Studies*, *49*(8), 1395–1401. https://doi.org/10.1111/j.1467-6486.2012.01080.x

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic Capabilities and Strategic Management. *Strategic Management Journal*, *18*(7), 509–533. https://doi.org/10.1093/0199248540.003.0013

Trinh-Phuong, T., Molla, A., & Peszynski, K. (2012). Enterprise systems and organizational agility: A review of the literature and conceptual framework. *Communications of the Association for Information Systems*, *31*(1), 167–193. https://doi.org/10.17705/1cais.03108

Tsen, E., Ko, R. K. L., & Slapnicar, S. (2022). An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce*, *32*(2), 153–174. https://doi.org/10.1080/10919392.2022.2068906

Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber Risk Assessment and Optimization: A Small Business Case Study. *IEEE ACCESS*, *11*, 44467–44481. https://doi.org/10.1109/ACCESS.2023.3272670 WE - Science Citation Index Expanded (SCI-EXPANDED)

Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: a critical success factor analysis. *Information and Computer Security*, *26*(2), 150–170. https://doi.org/10.1108/ICS-06-2017-0042

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers and Security*, *105*, 102239. https://doi.org/10.1016/j.cose.2021.102239

White, G. R. T., Allen, R. A., Samuel, A., Abdullah, A., & Thomas, R. J. (2022). Antecedents of Cybersecurity Implementation: A Study of the Cyber-Preparedness of U.K. Social

Enterprises. *IEEE Transactions on Engineering Management*, *69*(6), 3826–3837. https://doi.org/10.1109/TEM.2020.2994981

Wójcik, P., Obłój, K., & Buono, A. F. (2022). Addressing social concern through business-nonprofit collaboration: Microfoundations of a firm's dynamic capability for social responsibility. *Journal of Business Research*, *143*(January), 119–139. https://doi.org/10.1016/j.jbusres.2022.01.061

Wong, W. P., Tan, H. C., Tan, K. H., & Tseng, M.-L. (2019). Human factors in information leakage: mitigation strategies for information sharing integrity. *Industrial Management & Data Systems*, *119*(6), 1242–1267. https://doi.org/10.1108/IMDS-12-2018-0546

Woszczynski, A. B., & Green, A. (2017). Learning Outcomes for Cyber Defense Competitions. *Journal of Information Systems Education*, *28*(1), 21–42. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85062186549&partnerID=40&md5=3c832887241dbc9584ae27609f17f89a

Yauri, B. A., & Abah, J. (2016). Mitigating Security Threats in Virtualized Environments Bashir. *International Journal of Computer Science and Network Security*, *16*(1), 101–108. https://linkinghub.elsevier.com/retrieve/pii/S0278239104001284

Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, *19*(Spring), 1i. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85131902793&partnerID=40&md5=f5a7602b74b1274585228e64ed28b5bc

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers & Security*, *133*(June), 103412. https://doi.org/10.1016/j.cose.2023.103412

Zairul, M. (2020). A thematic review on student-centred learning in the studio education. *Journal of Critical Reviews*, *7*(2), 504–511. https://doi.org/10.31838/jcr.07.02.95

Zairul, M. (2021). The recent trends on prefabricated buildings with circular economy (CE) approach. *Cleaner Engineering and Technology*, *4*, 100239. https://doi.org/10.1016/j.clet.2021.100239

Zammani, M., & Razali, R. (2016). Information Security Management Success Factors. *Advanced Science Letters*, *22*(8), 1924–1929. https://doi.org/10.1166/asl.2016.7746

Zammani, M., Razali, R., & Singh, D. (2019). Factors contributing to the success of information security management implementation. *International Journal of Advanced Computer Science and Applications*, *10*(11), 384–391. https://doi.org/10.14569/IJACSA.2019.0101153

Zammani, M., Razali, R., & Singh, D. (2021). Organisational Information Security Management Maturity Model. *International Journal of Advanced Computer Science and Applications*, *12*(9), 668–678. https://doi.org/10.14569/IJACSA.2021.0120974

Zhen, J., Xie, Z., Dong, K., & Chen, L. (2021). Impact of negative emotions on violations of information security policy and possible mitigations. *Behaviour and Information Technology*, *0*(0), 1–13. https://doi.org/10.1080/0144929X.2021.1921029

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, *8*(4), 422–435. https://doi.org/10.1016/j.dcan.2021.07.006

Zrahia, A. (2018). Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. *Journal of Cybersecurity*, *4*(1), 1–16. https://doi.org/10.1093/cybsec/tyy008