Technology in Society 83 (2025) 103042

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Mapping the landscape of cybersecurity preparedness: A systematic review of non-technological determinants and consequences

Songkhun Nillasithanukroh [a], Chul Hyun Park [b,*], Jaejong Baek [c], Gail-Joon Ahn [c], Robert Richards [a]

[a] Clinton School of Public Service, University of Arkansas, 1200 President Clinton Avenue, Little Rock, AR, 72201, USA
[b] School of Public Policy, University of Maryland, Baltimore County, 1000 Hilltop Circle, Baltimore, MD, 21250, USA
[c] School of Computing and Augmented Intelligence, Arizona State University, 699 S. Mill Avenue, Tempe, AZ, 85281, USA

ARTICLE INFO

Keywords:
Cybersecurity preparedness
Assessment frameworks
Determinants
Consequences
Systematic literature review

ABSTRACT

Given the escalating technological reliance of organizations, the development of robust cybersecurity preparedness has become imperative to preempt and mitigate the spectrum of cyber threats that jeopardize operational integrity, data security, and reputational standing. Constructing an effective defense, however, remains challenging due to the prevailing tendency of existing cybersecurity preparedness assessment frameworks to prioritize technological solutions, often downplaying the critical roles of human, organizational, and environmental factors. Moreover, such frameworks frequently overlook the complex interplay among these domains and the full spectrum of consequential outcomes. This systematic literature review seeks to address these gaps by synthesizing empirical findings from a broad corpus of academic literature. The review elucidates the multifaceted determinants of cybersecurity preparedness, with particular emphasis on underexplored non-technological variables, and explicates the mechanisms by which these factors interrelate and ultimately influence preparedness outcomes. While the findings underscore the substantial impact of human, organizational, and environmental factors—often engaging in complex interactions with other variables—extant empirical research on these interdependencies remains limited. As a result, future research employing integrative frameworks is warranted to more comprehensively capture the dynamic interplay of determinants shaping cybersecurity preparedness. Further investigation is also necessary to delineate the range of long-term consequences of preparedness, thereby better informing organizations about the comprehensive value of cybersecurity investments.

1. Introduction

Cybersecurity preparedness has become a critical pillar of organizational strategy as the risks and impacts of cyber threats intensify across all sectors. The ongoing digital transformation of organizational operations has expanded both the attack surface and the sophistication of cyber threats, rendering organizations increasingly vulnerable to potentially severe consequences (Norris et al., 2019; Shandler & Gomez, 2023). Successful cyberattacks can result in operational downtime, service disruptions, reputational harm, and significant financial losses (Hawdon et al., 2023; Smith et al., 2023). In critical sectors such as healthcare and finance, breaches of sensitive information may lead to identity theft, fraud, and substantial legal or regulatory repercussions (Hasan et al., 2021; Tsen et al., 2022). Consequently, ongoing assessment and proactive enhancement of cybersecurity preparedness are essential to ensuring operational continuity, protecting stakeholder trust, and sustaining organizational resilience (Berlilana et al., 2021).

Over the past decade, a substantial body of research has emerged to define, measure, and improve organizational cybersecurity preparedness. Widely adopted standards and frameworks—such as the NIST Cybersecurity Framework and the ISO/IEC 27000 series—have served as foundational structures for assessment and continuous improvement, shaping both academic research and practical implementation (Taherdoost, 2022; Yeoh et al., 2023). Despite their importance, however, prevailing assessment approaches still face several notable limitations. Most assessment frameworks remain heavily oriented toward technological factors—such as infrastructure, detection, and response—while human, organizational, and environmental dimensions are

* Corresponding author.
E-mail addresses: snillasithanukroh@clintonschool.uasys.edu (S. Nillasithanukroh), chpark@umbc.edu (C.H. Park), jaejong@asu.edu (J. Baek), gahn@asu.edu (G.-J. Ahn), rcrichards@clintonschool.uasys.edu (R. Richards).

https://doi.org/10.1016/j.techsoc.2025.103042
Received 9 September 2024; Received in revised form 30 June 2025; Accepted 16 August 2025
Available online 20 August 2025

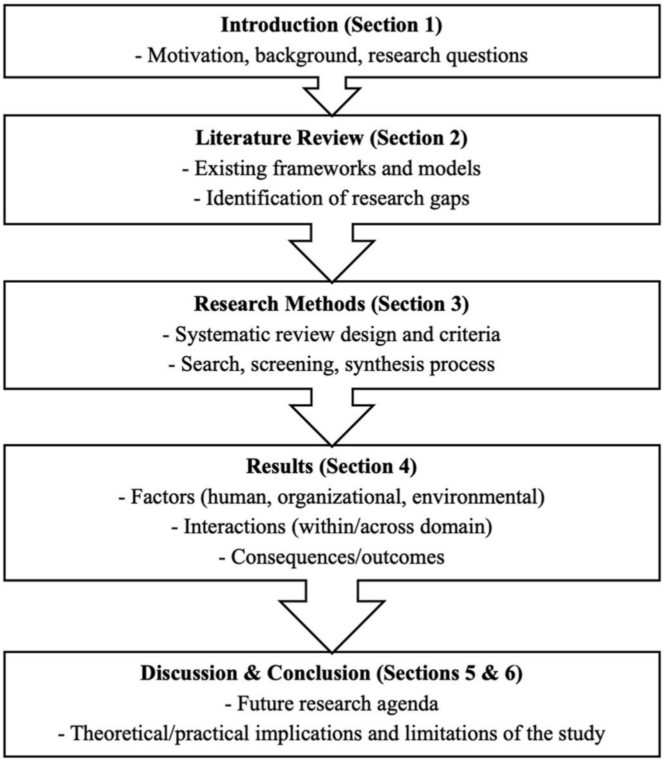
Introduction (Section 1)
- Motivation, background, research questions
Literature Review (Section 2)
- Existing frameworks and models
- Identification of research gaps
Research Methods (Section 3)
- Systematic review design and criteria
- Search, screening, synthesis process
Results (Section 4)
- Factors (human, organizational, environmental)
- Interactions (within/across domain)
- Consequences/outcomes
Discussion & Conclusion (Sections 5 & 6)
- Future research agenda
- Theoretical/practical implications and limitations of the study

Fig. 1. The Article's organization and structure.

often treated as peripheral or secondary (Chapman & Reithel, 2021; Hasan et al., 2021). Even as scholars increasingly advocate for more holistic models of cybersecurity preparedness (e.g., Hasan et al., 2021; Chapman & Reithel, 2021; Tsen et al., 2022), each of these efforts tends to focus on a limited subset of non-technological factors and frequently examine them in isolation from one another and from their technological counterparts. Similarly, these frameworks also tend to investigate only certain types of preparedness outcomes at a time.

As a result, several critical research gaps persist. First, most existing studies and frameworks do not adequately capture the comprehensive universe of preparedness determinants or the complex interactions among factors, both within and across technological and non-technological domains, and how these interdependencies shape cybersecurity preparedness. Second, prior frameworks and studies tend to examine the outcomes of cybersecurity preparedness in a fragmented manner, and lack a comprehensive framework that integrates outcomes across different time horizons (with the notable exceptions of Hasan et al., 2021; Chapman & Reithel, 2021). Third, there is a lack of synthesis regarding how contributing factors and outcomes may vary across organizational types, contexts, and environments, leaving practitioners with limited evidence-based guidance for comprehensive assessment and strategic resource allocation. These shortcomings underscore the urgent need for integrative frameworks and empirical evidence that can bridge these divides.

This study addresses these gaps through a systematic literature review that consolidates and synthesizes empirical findings on the multi-dimensional determinants and outcomes of cybersecurity preparedness. By identifying a broad range of non-technological factors—and, crucially, how these elements interact within and across domains—as well as bringing together the immediate, intermediate, and long-term outcomes associated with preparedness, this review advances a more holistic and nuanced understanding of organizational cybersecurity preparedness, allowing for the development of assessment frameworks that are more responsive the cyber threats. The added value of this study lies in the explicit articulation of interdependencies that previous frameworks have only partially addressed, along with the comprehensive mapping of both immediate and long-term organizational outcomes.

Guided by this aim, the systematic literature review is organized around two core research questions.

- RQ1: What non-technological factors influence an organization's cybersecurity preparedness, and how do these factors interact within and across domains (technological, human, organizational, and environmental) to shape preparedness?
- RQ2: What are the immediate, intermediate, and ultimate impacts and outcomes associated with varying levels of cybersecurity preparedness?

To aid navigation and provide structural clarity, Fig. 1 offers a visual overview of the article's organization and main themes. Specifically, Section 2 reviews the evolution of existing assessment frameworks and models and identifies their limitations. Section 3 details the systematic review methodology, including the literature search and screening process, data extraction, and thematic synthesis methods. Following this, Section 4 synthesizes findings regarding the non-technological determinants and consequences of cybersecurity preparedness, with particular emphasis on their interactions. The article concludes by outlining a future research agenda and discussing practical implications for both scholars and practitioners in Sections 5 and 6.

2. Background and motivation: review of existing assessment frameworks

Over the past decade, numerous frameworks have been developed and applied to assess the cybersecurity preparedness of organizations. In preparing this article, we systematically reviewed more than 30 prior studies that either proposed new assessment frameworks or empirically tested existing ones. From this review, two major themes emerged: (1) the integration of established standards into assessment frameworks; and (2) the adoption of holistic approaches to cybersecurity assessment.

2.1. Integration of established standards into assessment frameworks

A predominant approach in the literature involves adapting widely recognized standards and measurement tools for the assessment of cybersecurity preparedness (Yeoh et al., 2023; Verdugo & Rodríguez, 2020). Among the existing studies, several key standards have been most frequently utilized and adapted across diverse sectors:

The NIST Cybersecurity Framework (CSF), developed by the U.S. National Institute of Standards and Technology, is widely recognized for its comprehensive structure. The framework organizes cybersecurity activities into six core functions: "Govern," "Identify," "Protect," "Detect," "Respond," and "Recover" (Ahouanmenou et al., 2023; Antunes et al., 2022; Delgado et al., 2021). Each function is further divided into categories and subcategories that specify measurable outcomes and implementation activities. The NIST CSF is valued for its flexibility and adaptability to various organizational contexts, from the public sector to critical infrastructure and private enterprises.

Another frequently cited framework is the ISO/IEC 27000 family, developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This suite of standards focuses on the development, implementation, and continual improvement of Information Security Management Systems (ISMS) (Bahuguna et al., 2019; Barraza de la Paz et al., 2023). Specifically, ISO/IEC 27001 sets forth requirements for establishing and maintaining an ISMS, while ISO/IEC 27004 provides guidelines for monitoring, measurement, analysis, and evaluation of ISMS performance.

A significant number of assessment studies also utilize the Capability Maturity Model Integration (CMMI)—originally developed for software process improvement—or its derivatives for cybersecurity evaluation

(Aliyu et al., 2020; Bernardo et al., 2025). For instance, the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2) is widely applied to assess organizational cybersecurity capabilities. The maturity model typically defines five levels: (1) Initial, (2) Managed, (3) Defined, (4) Quantitatively Managed, and (5) Optimized. Many evaluations extract core factors from NIST or ISO standards and then apply a maturity model to qualitatively and quantitatively assess the organization's cybersecurity posture (Garba et al., 2020).

This integration of established standards and maturity models into assessment frameworks enables organizations to benchmark their cybersecurity preparedness, identify gaps, and develop roadmaps for improvement. Furthermore, the use of recognized standards such as NIST CSF and ISO/IEC 27000 series in assessment frameworks facilitates compliance with regulatory requirements and promotes the adoption of best practices across sectors.

Empirical examples illustrate these approaches in context. For instance, Aliyu et al. (2020) developed a comprehensive cybersecurity assessment framework for higher education institutions by identifying 15 essential cybersecurity components derived from established standards such as ISO/IEC 27001 and the European Union Agency for Cybersecurity (ENISA) audit and assessment framework. These components were grouped into three modified NIST Cybersecurity Framework (CSF) core functions—Identify, Protect & Detect, and Respond & Recover—and measured using a six-level maturity model, from Level 0 (Incomplete) to Level 5 (Optimizing). The framework's practical applicability was validated through qualitative interviews with cybersecurity experts in the higher education sector.

Similarly, Bernardo et al. (2025) combined expert input and empirical data to construct a cybersecurity preparedness index. After surveying experts to determine the relative importance of NIST CSF core functions, categories, and subcategories, they assigned weights to different components and selected approximately 100 survey items aligned with the NIST CSF. Survey data collected from four companies, together with these weights, were integrated to create a context-sensitive cybersecurity preparedness index that reflects organizational readiness.

In contrast, Neri et al. (2022) focused on Small and Medium-sized Enterprises (SMEs) in Italy, employing the Delphi method to design an assessment questionnaire based on a synthesis of NIST, ISO/IEC, and the Italian Institute of Statistics standards. Survey responses from over 700 SMEs, supplemented by semi-structured interviews, provided a detailed picture of both strengths and weaknesses in SME cybersecurity practices. Their findings emphasized that, despite progress in areas like critical information security management, many SMEs still lack formal, organization-wide cybersecurity policies.

Taken together, these studies reflect a growing emphasis on adapting established standards to sector-specific contexts and validating assessment frameworks with empirical evidence. This trend not only enhances the relevance and rigor of cybersecurity preparedness evaluations but also supports organizations in identifying tailored strategies for improvement.

2.2. *A holistic approach to Assessing Cybersecurity Preparedness*

While the integration of established standards has provided a strong foundation for cybersecurity assessment, a growing body of research advocates for more holistic frameworks—those that incorporate not only technological, but also organizational, human, and environmental factors. Latino and Menegoli (2022) did not seek to create an assessment model, but their efforts provide a reference framework useful for scholars and practitioners to design their own security evaluation projects. Their framework takes into account both human and technological (software, hardware, and network) factors to identify various cyber threats (phishing, spyware, ransomware, etc.) and countermeasures (firewalls, user activity monitoring, access control, etc.).

Georgiadou et al. (2022) conducted a comprehensive review of commonly utilized security standards and models to develop a cybersecurity culture framework for organizational assessment. They define security culture as a state or process wherein every member of the organization is "aware of the relevant security risks and preventative measures, assumes responsibility, and takes steps to improve the security of their information systems and networks" (p. 452). Their analysis identified two high-level components—"Organizational" and "Individual"—and ten sub-components spanning these categories. The "Individual" component includes factors such as attitude, behavior, and competency, while the "Organizational" component covers access and trust, security governance, and operations. Ultimately, they proposed 52 specific sub-components across the ten categories, providing a nuanced and human-centric framework for evaluating cybersecurity culture and preparedness.

Similarly, Aldabjan et al. (2024) undertook a literature review to identify a variety of human, organizational, operational, and external factors that influence an organization's incident response preparedness. Each high-level factor comprises several sub-factors—eleven in total. For example, the "human" category encompasses security culture, training and awareness, and communication, while "external" factors address third-party relationships and collaborative incident response. A notable contribution of this study is the mapping of interrelationships among these sub-factors, offering a basis for hypothesis development and empirical testing of incident response preparedness.

Photipatphiboon et al. (2025) employed the Technology, Organization, and Environment (TOE) framework to conceptualize and empirically test factors influencing organizational cybersecurity preparedness in Thailand. Their study collected survey data from 400 respondents to examine how technological, organizational, and environmental preparedness (as independent variables) impact cybersecurity awareness (as a mediator), which in turn affects cybersecurity compliance behavior and knowledge-sharing intention (dependent variables). Their findings indicate that preparedness in these three areas is positively associated with cybersecurity awareness, which itself is a significant predictor of compliance and knowledge-sharing behaviors—particularly in developing country contexts.

Chapman and Reithel (2021) developed the Practice and Awareness Cybersecurity Readiness Model (PACRM) to test the relationships among individual, organizational, and technical factors and cybersecurity preparedness to detect, prevent, and recover from cyberattacks. Their determinants include factors such as prior cybersecurity experience, personal risk avoidance, network monitoring, physical access controls, preventive software measures, and cybersecurity awareness. Using survey data and structural equation modeling, they tested 26 hypotheses, ultimately finding empirical support for 11, particularly those related to prior experience, awareness, network monitoring, and backup policies.

Taken together, these studies illustrate the increasing sophistication and scope of cybersecurity preparedness frameworks, emphasizing the interplay between human, organizational, and technological factors. Such holistic approaches are essential for understanding and improving the full spectrum of organizational cybersecurity readiness in an era of evolving threats.

2.3. *Research gaps in the literature*

Our comprehensive review of existing assessment frameworks, empirical studies, and literature reviews reveals several critical research gaps in the literature on cybersecurity preparedness. First, the majority of current assessment frameworks are grounded in established standards, such as NIST and ISO/IEC (e.g., Aliyu et al., 2020; Bernardo et al., 2025). Although these standards and the resulting assessment frameworks increasingly acknowledge some non-technological components—such as organizational structure or user awareness—they continue to place primary emphasis on technological controls and safeguards. As a result, important non-technological factors—including human, organizational, and environmental dimensions—still remain underemphasized in these frameworks. Several recent studies and literature reviews have begun to address this limitation by suggesting and developing more comprehensive assessment frameworks. For example, Hasan et al. (2021) proposed a model that integrates technological, organizational, and environmental factors. However, each of these newer frameworks tends to address only a subset of the broad spectrum of contextual influences that may affect cybersecurity preparedness. There is still a lack of frameworks grounded in systematic investigations into the full range of human, organizational, and environmental variables that could influence cybersecurity preparedness.

Furthermore, even among studies, frameworks, and reviews that incorporate and address non-technological elements, few systematically and comprehensively examine how factors, both technological and non-technological, interact to influence cybersecurity preparedness, leaving the existing research landscape on interactions fragmented. While Aldabjan et al. (2024) and Chapman and Reithel (2021) highlight the interrelations among factors, they fall short of providing comprehensive models that capture the full range of interdependencies critical to effective preparedness.

Second, there is a notable lack of theory development and hypothesis testing in the assessment literature. This gap is closely related to the narrow focus described above: most prior studies identify relevant factors—especially technological ones—from established standards and conduct descriptive assessments of an organization's cybersecurity status. However, few studies move beyond description to rigorously theorize and empirically test the relationships among these factors, or to evaluate their impact on concrete cybersecurity outcomes (e.g., Chapman & Reithel, 2021; Photipatphiboon et al., 2025). As a result, the field lacks a robust body of theory and empirical evidence that explain how both technological and non-technological factors interact and contribute to effective cybersecurity. This finding is congruent with Khan et al. (2022) who conducted a systematic review of cybersecurity behavior and concluded that current literature lacks the theoretical conceptualization and rigorous operationalization of key factors related to cybersecurity behavior.

Third, another important gap in existing research on preparedness frameworks pertains to the comprehensive identification and testing of these frameworks in relation to the outcomes and effects of cybersecurity preparedness. Prior theoretical or empirical research and literature reviews considered a variety of outcomes, often in isolation, and primarily focused on immediate impacts. These outcomes and effects include data theft (Khan et al., 2021), financial loss (Smith et al., 2023), and reduced confidence (Hawdon et al., 2023). However, to the best of our knowledge, no existing study has systematically identified and synthesized the full spectrum of potential outcomes of cybersecurity preparedness or developed an assessment framework that incorporates immediate, intermediate, and long-term outcomes.

The present study seeks to address these gaps and contribute to the development of a more holistic and evidence-based understanding of organizational cybersecurity preparedness.

3. Research approach: systematic literature review

This section outlines the systematic methodology employed to rigorously synthesize empirical findings on the determinants and consequences of cybersecurity preparedness. A thematic synthesis approach (Xiao & Watson, 2019) was adopted to identify, categorize, and interpret recurring patterns and themes across a diverse literature base. This method is particularly well-suited to interdisciplinary topics such as cybersecurity preparedness, where relevant research spans multiple fields and levels of analysis.

3.1. Setting objectives and formulating research questions

Clear objectives and research questions were established to guide the systematic review, grounded in the contemporary landscape of cybersecurity preparedness scholarship. The primary goal was to synthesize and analyze empirical studies examining the determinants, with special attention to non-technological factors and their interactions within and across domains, and consequences of cybersecurity preparedness. The research questions focused the investigation and facilitated a nuanced understanding of both the complexity and interdependence of these factors. Rather than only examining determinants in isolation, the review also sought to uncover their interactions—how they reinforce or constrain one another—and how these dynamics collectively shape organizational readiness. Additionally, the review examined the full spectrum of outcomes, including those that may not be immediately observable but are nevertheless critical to understanding preparedness outcomes.

Table 1
Search terms used on databases for literature search based on PICO framework.

Topic	Databases	Search Strings Utilized in the Title, Abstract, and Keywords
Factors Influencing Cybersecurity Preparedness	Web of Science, Google Scholar, Scopus	(“cybersecurity preparedness” OR “cyber readiness” OR “cyber resilience” OR “information security preparedness") AND (“factor*” OR “driver*” OR “determinant*" OR “influenc*” OR “predictor*" OR “barrier*”) AND (“organization*” OR “enterprise*” OR “institution*" OR “firm*" OR “agency")
Interactions Between Determinants of Preparedness	Web of Science, Google Scholar, Scopus	(“cybersecurity preparedness” OR “cyber readiness” OR “cyber resilience” OR “information security preparedness") AND (“outcome*” OR “impact*” OR “effect*" OR “result*” OR “consequence*”) AND (“organization*” OR “institution*” OR “firm*” OR “enterprise”)
Consequences and Outcomes of Cybersecurity Preparedness	Web of Science, Google Scholar, Scopus	(“cybersecurity preparedness” OR “cyber readiness” OR “cyber resilience” OR “information security preparedness”) AND (“interaction*” OR “interrelat*” OR “interdependen*” OR “moderator*” OR “mediator*” OR “cross-domain”) AND (“factor*" OR “driver*" OR “determinant*" OR “influenc*” OR “predictor*”OR “barrier*”) AND (“organization*” OR “institution*” OR “agency”)

3.2. Systematic search for relevant literature

A systematic search strategy, grounded in the PICO framework (Population, Intervention, Comparison, Outcome), was employed to identify relevant studies (Eriksen & Frandsen, 2018). This structure enabled the use of comprehensive search terms that captured a wide range of studies addressing contributing factors and cybersecurity-related outcomes (see Appendix A for the PICO structure). Search strings, detailed in Table 1, were applied to the title, abstract, and keywords fields.

The initial search was conducted in October 2023 and updated in February 2025. Coverage spanned disciplines including social sciences, business, information systems, law, and technology to capture a diversity of perspectives on organizational cybersecurity. Searches were limited to English-language, peer-reviewed journal articles and conference proceedings published between January 2016 and December 2024. The primary search using Web of Science—covering over 20,000 journals—yielded 683 articles (Aksnes & Sivertsen, 2019). To ensure full

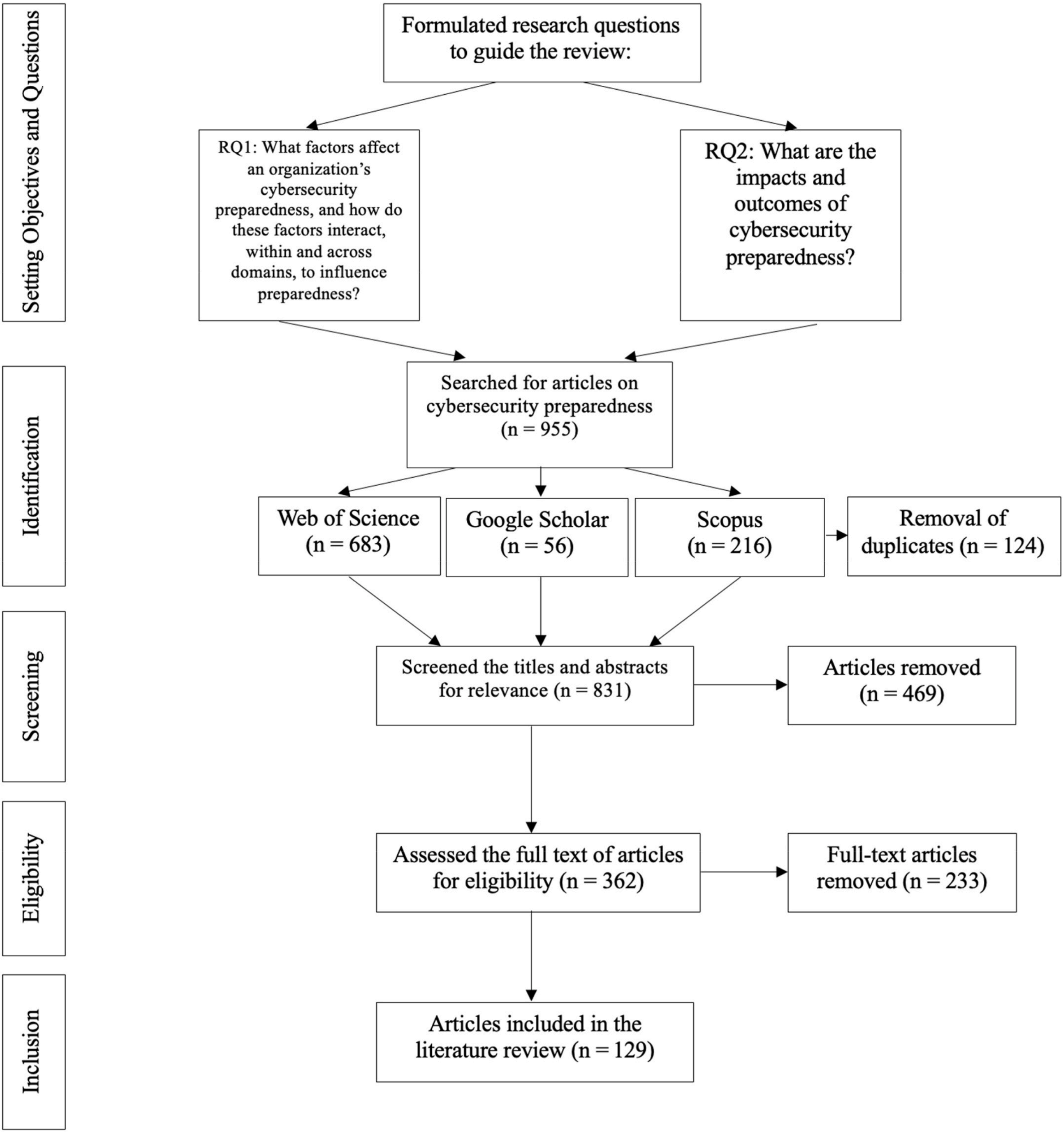
Setting Objectives and Questions
Formulated research questions to guide the review:
RQ1: What factors affect an organization's cybersecurity preparedness, and how do these factors interact, within and across domains, to influence preparedness?
RQ2: What are the impacts and outcomes of cybersecurity preparedness?
Identification
Searched for articles on cybersecurity preparedness (n = 955)
Web of Science (n = 683)
Google Scholar (n = 56)
Scopus (n = 216)
Removal of duplicates (n = 124)
Screening
Screened the titles and abstracts for relevance (n = 831)
Articles removed (n = 469)
Eligibility
Assessed the full text of articles for eligibility (n = 362)
Full-text articles removed (n = 233)
Inclusion
Articles included in the literature review (n = 129)

Fig. 2. Prisma flow diagram.

coverage and minimize database bias, additional searches were conducted in Scopus and Google Scholar, yielding 216 and 56 additional articles, respectively (Gehanno et al., 2013). Among the 955 articles initially identified, 124 were duplicates, leaving 831 unique articles.

3.3. Relevance and quality assessment

To ensure rigor and relevance, a two-stage screening process consistent with PRISMA guidelines was implemented. First, the titles and abstracts of all identified articles were screened for relevance according to the following criteria.

- The study empirically investigated factors influencing organizational cybersecurity preparedness, including interactions both within and across domains.
- The study provided empirical evidence on the outcomes or impacts of cybersecurity preparedness—whether immediate, intermediate, or long-term, and whether tangible or intangible.

Only empirical studies—quantitative, qualitative, or mixed

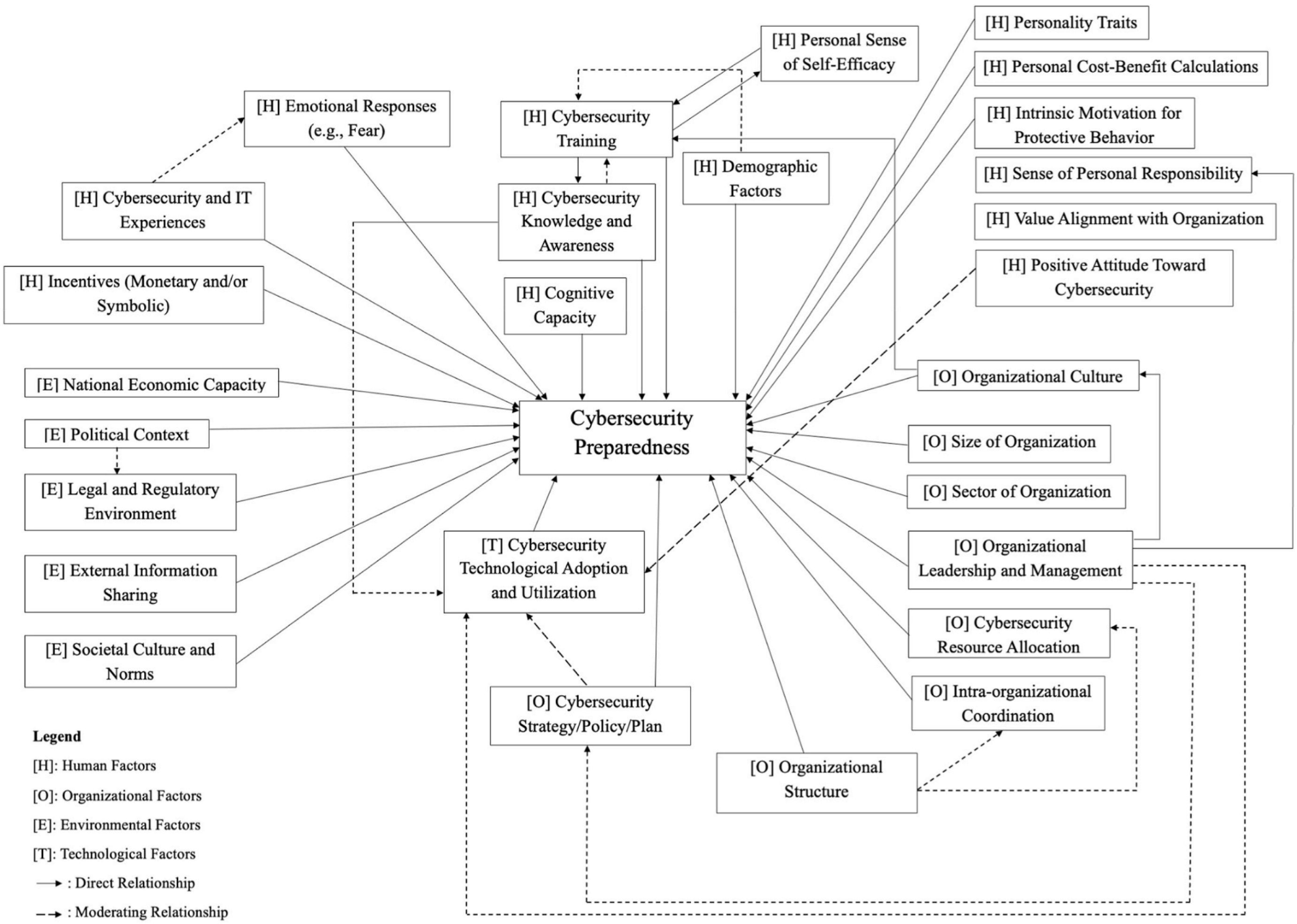
[H] Personality Traits
[H] Personal Cost-Benefit Calculations
[H] Intrinsic Motivation for Protective Behavior
[H] Sense of Personal Responsibility
[H] Value Alignment with Organization
[H] Positive Attitude Toward Cybersecurity
[H] Personal Sense of Self-Efficacy
[H] Emotional Responses (e.g., Fear)
[H] Cybersecurity Training
[H] Demographic Factors
[H] Cybersecurity and IT Experiences
[H] Cybersecurity Knowledge and Awareness
[H] Incentives (Monetary and/or Symbolic)
[H] Cognitive Capacity
[E] National Economic Capacity
[E] Political Context
[E] Legal and Regulatory Environment
[E] External Information Sharing
[E] Societal Culture and Norms
Cybersecurity Preparedness
[O] Organizational Culture
[O] Size of Organization
[O] Sector of Organization
[O] Organizational Leadership and Management
[O] Cybersecurity Resource Allocation
[O] Intra-organizational Coordination
[O] Organizational Structure
[O] Cybersecurity Strategy/Policy/Plan
[T] Cybersecurity Technological Adoption and Utilization
Legend
[H]: Human Factors
[O]: Organizational Factors
[E]: Environmental Factors
[T]: Technological Factors
: Direct Relationship
: Moderating Relationship

Fig. 3. Framework for assessing cybersecurity preparedness.

methods—were retained to ensure the synthesis focused on evidence-based findings. Purely theoretical or conceptual works were excluded to prioritize practical, data-driven insights. After abstract screening, 469 did not meet the above criteria, leaving 362 articles for full-text review.

In the second stage, full-text screening was conducted using a quality assessment framework adapted from Xiao and Watson (2019) and Batini et al. (2009). Studies were included if they.

- Clearly stated research questions or objectives;
- Employed a well-described, appropriate empirical research design;
- Used valid and reliable data sources and a transparent, replicable methodological approach;
- Provided analyses and interpretations logically aligned with their aims.

Studies were excluded if cybersecurity preparedness was not a central focus, if they lacked methodological clarity, or if they failed to meet quality standards. After this assessment, 233 additional studies were excluded, yielding 129 empirical studies for data extraction and thematic synthesis.

For quality control, both stages of review were conducted independently by two authors. Each author assessed the abstracts and full texts using assessment rubric focused on relevance, methodological transparency, conceptual clarity, and empirical rigor. Any discrepancies in inclusion decisions were discussed and resolved through consensus to minimize individual bias and ensure methodological rigor.

The complete process is illustrated in Fig. 2 (PRISMA flow diagram). Our PRISMA protocol was not pre-registered, as this practice is uncommon in social sciences, including business administration, political science, and public administration. We acknowledge that pre-registration can offer numerous academic benefits by increasing research credibility and promoting transparency.

3.4. Data extraction and thematic synthesis

For each included study, basic metadata were extracted (see Table B.1, Appendix B). The core of data extraction focused on a thematic synthesis of empirical content related to (1) factors contributing to cybersecurity preparedness, (2) interactions among these factors, and (3) organizational outcomes associated with preparedness.

A deductive coding strategy (Creswell & Creswell, 2023), informed by the research questions, structured the content analysis. Four major domains of contributing factors were coded: technological, human, organizational, and environmental. Interactions among factors—within and across domains—were also coded to capture reinforcing, counteracting, or mediating influences. Outcomes were categorized as immediate, intermediate, or long-term. To ensure reliability and reduce individual coder bias, two authors independently coded all studies using a structured codebook developed for this review. This dual-coder approach promoted inter-coder consistency and enabled the identification and resolution of discrepancies through consensus discussion. The coding process involved three stages.

- Open coding: Extraction of all relevant text segments on contributing factors, mechanisms, and outcomes of cybersecurity preparedness.
- Axial coding: Open codes were analyzed to group them into higher-order categories, organized by domain of contributing factors, patterns of interaction among factors, and types of outcomes.
- Selective coding: Identification of cybersecurity preparedness as the central construct, mapping relationships among categories, and integrating themes into a cohesive explanatory narrative.

Thematic synthesis (Xiao & Watson, 2019) enabled the integration of disparate findings into a coherent narrative, illuminating the pathways linking organizational conditions, cybersecurity preparedness, and resulting outcomes.

4. Results from the systematic literature review

This section presents the findings from our thematic synthesis of empirical studies, focusing on three key areas: (1) the contributing factors that shape organizational cybersecurity preparedness, with particular attention to under-examined non-technological domains—namely, human, organizational, and environmental dimensions; (2) the interactions among these factors, both within and across domains; and (3) the outcomes and consequences associated with cybersecurity preparedness.

Rather than simply listing contributing factors, this synthesis integrates them into broader thematic categories and emphasizes the mechanisms through which these factors operate. This approach allows us to trace how specific inputs influence preparedness, or interact with other factors, to shape organizational readiness. We also examine how cybersecurity preparedness leads to various short-, intermediate-, and long-term organizational outcomes. While we conducted data extraction and thematic analysis of 129 studies, some content overlap was present among them. Therefore, we prioritized citing the most recent literature on each topic, resulting in 109 studies cited here. The full list of studies analyzed is provided in Appendix C.

Combining insights extracted from the literature on their relation to the concept of cybersecurity preparedness, Fig. 3 presents a conceptual framework mapping the determinants of cybersecurity preparedness, illustrating how factors from different domains directly and interactively influence an organization's cybersecurity readiness. Solid arrows represent direct relationships, dashed arrows indicate moderating effects, and the directional flow of arrows illustrates how factors influence cybersecurity preparedness, either directly, by shaping preparedness themselves, or indirectly, by mediating through another variable.

4.1. Factors contributing to cybersecurity preparedness

This section addresses the first analytical dimension: the direct contributions of individual factors to cybersecurity preparedness. We identified and synthesized empirical evidence on a range of specific inputs and examined how these enable or constrain preparedness. These inputs form the foundational capacities and contextual conditions that determine an organization's ability to anticipate, prevent, and respond to cyber threats. The findings in this section responds to the first part of RQ1 on the non-technological factors that influence an organization's cybersecurity preparedness. We identify and analyze contributing factors within three under-examined non-technological domains, human, organizational, and environmental.

While the importance of technological infrastructure is widely acknowledged, the empirical literature on non-technological determinants—such as human, organizational, and environmental factors—remains comparatively underdeveloped. Addressing this gap, our review prioritizes these non-technological domains, recognizing their important role in shaping cybersecurity outcomes and advancing a better understanding of organizational preparedness.

4.1.1. Human factors

Human factors emerged as indispensable, non-technological elements of cybersecurity preparedness. Our thematic synthesis identified seven categories of human factors: (1) cybersecurity knowledge and training, (2) experience and tenure, (3) cognitive capacity, (4) intrinsic drivers, (5) emotional responses, (6) demographic factors, and (7) incentive structures.

First, cybersecurity knowledge forms a foundational input into preparedness, by shaping cybersecurity behaviors. Empirical studies consistently show that limited knowledge among staff increases vulnerability to cyber incidents, whereas greater cybersecurity knowledge improves threat awareness, response capabilities, adherence to policies, and overall security practices (Alhalafi & Veeraraghavan, 2022; Althobaiti, 2021; Ani et al., 2019; Eliza et al., 2024; Li et al., 2023; Rodriguez-Priego et al., 2020). Importantly, an organization's preparedness is often only as strong as its weakest link; thus, limited awareness among even a few individuals can significantly undermine overall cybersecurity readiness (Ani et al., 2019).

To address this, the NIST framework emphasizes the necessity of regular cybersecurity training—not only to educate individuals about cyber threats and best practices but also to sustain vigilance regarding evolving risks and refresh on organizational protocols (Georgiadou et al., 2021; Kioskli et al., 2023; Nystad et al., 2021; Pinto, 2022; Sapanca & Kanbul, 2022). Training is most effective when it is in-depth, routinely updated to reflect the latest threats, and tailored to individuals' specific roles within the organization (Goupil et al., 2022; Tsado et al., 2024, pp. 1–5). Moreover, general IT education further enhances preparedness by enabling staff to understand system functionality, identify deviations from normal operations, and contextualize cybersecurity practices (AlMindeel & Martins, 2020).

Second, experience and tenure—particularly in IT or cybersecurity-related roles—contributes significantly to organizational preparedness. Employees who have personally encountered cyber incidents or have spent substantial time working in relevant IT settings tend to recognize threats more readily, adapt quickly to evolving threats, and formulate innovative responses (Chapman & Reithel, 2021; Fusi et al., 2023; Kostyuk & Wayne, 2021; Li et al., 2019; Nam, 2019; Smith et al., 2021).

Third, cognitive capacity—the ability to process information and sustain attention—is also crucial. When employees are overloaded by excessive training, awareness messages, and compliance demands, they may experience mental fatigue. This fatigue impairs their ability to filter out irrelevant stimuli and detect potential threats, ultimately weakening adherence to security protocols (Kim & Kim, 2024; Smith et al., 2021). Organizations can counteract this by adopting human-centered design strategies, such as simplifying user interfaces, minimizing repetitive tasks, and automating secure behaviors when feasible.

Fourth, intrinsic drivers—including attitudes, motivation, sense of responsibility, alignment with organizational values, personality traits, perceived costs and benefits, and self-efficacy—profoundly shape individual cybersecurity behavior. Positive attitudes toward cybersecurity, high intrinsic motivation, and a sense of accountability are linked to greater vigilance and adherence to security practices (AlMindeel & Martins, 2020; Neigel et al., 2020; Onumo et al., 2021; Posey & Folger, 2020; Vafaei-Zadeh et al., 2019). Personality traits such as conscientiousness, associated with greater attention to detail, and extroversion, linked to stronger interpersonal engagement, can also influence how individuals process cybersecurity information and coordinate responses to cyber threats (Li et al., 2023).

Value alignment between employees and organizational cybersecurity goals promotes voluntary compliance, greater engagement, and the normalization of secure practices (Hasan et al., 2021). Employees are more likely to embrace policies they perceive as consistent with their own ethical standards, which strengthens security culture. Likewise, employees' cost-benefit assessments regarding cybersecurity practices—perceiving secure behaviors as inconvenient or yielding little benefit—can reduce compliance and undermine the consistency of positive security practices across the organization (Hasani et al., 2023; Yudhiyati et al., 2021). Finally, high self-efficacy—the belief in one's ability to effectively implement secure behaviors—supports confident action, rapid incident response, and sustained engagement with security routines (Hasani et al., 2023).

Fifth, emotional responses, particularly fear, can directly influence cybersecurity preparedness. Credible, detailed information about potential cyber harms triggers concern, which can motivate immediate action and strict adherence to protocols (Schuetz et al., 2020; Sylvester, 2022). However, if secure practices are seen as inconvenient, the effect of fear may be overridden, leading employees to prioritize short-term personal benefits over long-term security (Ng et al., 2021). Messaging that pairs emotional appeals with actionable guidance and organizational support is therefore most effective in inducing protective behavior (Rodriguez-Priego et al., 2020).

Sixth, demographic factors such as age, gender, and educational background influence organizational cybersecurity preparedness by shaping digital literacy, risk perceptions, and responsiveness to training. Research findings in this area are mixed: younger employees may have greater fluency with digital tools but also exhibit higher risk-taking behaviors; older employees may be more risk-averse but less adaptable to new technologies (Alrababah et al., 2024; Anwar et al., 2017; Hossain et al., 2022, pp. 309–314; Lee & Kim, 2020; Li et al., 2023; Neigel et al., 2020; Sapanca & Kanbul, 2022). Higher educational attainment, particularly in STEM fields, is associated with greater understanding of cybersecurity risks and improved capacity to implement security measures (Allodi et al., 2020; Alrababah et al., 2024; Soylu et al., 2021, pp. 1–7).

Seventh, incentive structures, whether monetary (e.g., bonuses, penalties) or symbolic (e.g., recognition, awards), shape motivation and accountability. When organizations implement clear, consistent incentives that reward secure behaviors and penalize risky actions, they promote the internalization of cybersecurity practices, helping embed them as a routine part of conduct (AlMindeel & Martins, 2020).

In sum, human factors serve as indispensable drivers of organizational cybersecurity preparedness. Each factor directly shapes employees' abilities to recognize threats, make informed decisions, and reliably apply secure practices. When aligned with organizational strategy, these factors enhance both individual and collective readiness. Conversely, neglecting human factors introduces vulnerabilities that even the most sophisticated technological systems cannot offset. These findings underscore the importance of integrating human-centered strategies into every phase of preparedness planning. Table D.2 in Appendix D summarizes the human factors influencing cybersecurity preparedness.

4.1.2. *Organizational factors*

Organizational factors form the infrastructure of cybersecurity preparedness, influencing both an organization's capacity for action and its ability to translate policies and resources into meaningful preparedness outcomes. These factors create the conditions under which cybersecurity readiness can be developed, sustained, and improved. Through thematic synthesis, we identified seven key organizational dimensions: (1) leadership, (2) culture, (3) resource allocation, (4) organizational structure, (5) planning, (6) coordination, and (7) sectoral context.

Leadership is a foundational driver of preparedness. When senior leaders clearly communicate that cybersecurity is a core organizational value, they elevate its importance across all levels, ensuring it is not relegated to the IT department but embedded as a cross-cutting priority within strategic decision-making, risk management, and organizational planning (Abraham et al., 2019; Aldabjan et al., 2024; Al-ma'aitah, 2022; Auffret et al., 2017; De La Cruz et al., 2024, pp. 403–408; Hasan et al., 2021; Onumo et al., 2021). Leadership exerts its influence primarily through agenda-setting and resource mobilization—determining which initiatives are prioritized, funded, and institutionally supported. Elevating cybersecurity to a boardroom-level concern increases the likelihood of consistent funding, integration into performance metrics, and strategic workforce planning (Al-Kumaim & Alshamsi, 2023). Leadership also plays a critical role in institutionalizing policies, translating strategic goals into enforceable rules and operational procedures. Finally, leaders who visibly champion cybersecurity foster an environment of shared responsibility and empower employees to adopt secure behaviors, ultimately strengthening the organization's security posture (Al-ma'aitah, 2022; Onumo et al., 2021).

Organizational culture is equally crucial, shaping how employees perceive and respond to cyber risks. While leadership sets the agenda, culture determines whether those priorities are internalized and enacted at all levels. A robust cybersecurity culture, where secure behaviors are valued and reinforced, creates an environment in which vigilant and responsible actions become habitual (Dong et al., 2024; Hasan et al., 2021; Kessler et al., 2020; Li et al., 2019; Onumo et al., 2021). Employees who see cybersecurity as a shared norm are more likely to comply with protocols, even without supervision. Additionally, cultures emphasizing collective responsibility promote mutual monitoring and accountability, facilitating early detection and mitigation of vulnerabilities. Importantly, cultures that frame employees as part of the solution—not as weak links—create psychological safety, encouraging incident reporting without fear of reprisal (Chatterjee & Leslie, 2024; Zimmermann & Renaud, 2019). Furthermore, strong cybersecurity cultures promote knowledge sharing and collaboration, extending the reach of individual expertise and enabling adaptive responses to emerging threats (AlMindeel & Martins, 2020).

Resource allocation serves as the bridge that connects leadership intent and cultural values with the tangible capacity for preparedness. Sustained investment in cybersecurity tools, personnel, infrastructure, and training significantly enhances the organization's capacity to prevent, detect, and respond to cyber threats (Auffret et al., 2017; Berlilana et al., 2021; Chidukwani et al., 2024; Dinkova et al., 2023; Hasan et al., 2021; Neri et al., 2024; Tsado et al., 2024, pp. 1–5; White et al., 2022; Yudhiyati et al., 2021). The impact of resource allocation is seen in the operational capability of well-funded organizations: they deploy up-to-date technologies, employ specialized staff, and maintain monitoring systems for rapid threat detection and incident response. However, investment must be strategically targeted. Aligning expenditures with risk exposure, workforce needs, and technological requirements yields stronger preparedness than ad hoc or reactive investments (Kissoon, 2020). Strategic investment recognizes that resources invested in one area often have spillover benefits in others (Armenia et al., 2019). Conversely, resource constraints can curb innovation and hinder organizational learning, due to fear of wasting scarce resources on unproven cybersecurity measures (Fusi et al., 2023).

Strategic planning—specifically, the development, continual refinement, and enforcement of a formal cybersecurity plan or policy—is the roadmap for translating resources into structured, organization-wide action (Chowdhury et al., 2023; Dong et al., 2024; He et al., 2022; Pinto, 2022; Pollini et al., 2022; Sullivan et al., 2023; Tsado et al., 2024, pp. 1–5). Formalized plans, as emphasized by frameworks like the NIST CSF, define priorities, outline objectives, delineate responsibilities, and establish protocols for prevention, detection, response, and recovery. Such plans reduce ambiguity, promote operational coherence, and ensure that employees understand how their roles contribute to cybersecurity objectives. Strategic plans are most effective when developed collaboratively with employees, tailored to operational realities, and embedded within workflows—enhancing clarity, reducing friction, and increasing buy-in (Li et al., 2019; Pham et al., 2019). Plans must also be dynamic—regularly updated in response to evolving threats and supported by performance evaluation and feedback mechanisms that enable continuous improvement and adaptive resilience (Porter & Tan, 2023).

Organizational structure, particularly the degree of centralization in cybersecurity governance, shapes the effectiveness of cybersecurity practices. Centralized governance, often led by a Chief Information Security Officer (CISO), consolidates authority, clarifies accountability, and enables unified decision-making (Auffret et al., 2017; Caldarulo et al., 2022; Neri et al., 2024). This approach minimizes redundancy, reduces fragmentation, and ensures consistency in protocol implementation. Centralized organizational structures facilitate uniform training, system configuration, and communication, while decentralized structures risk silos, inconsistencies, and thereby delayed response (Abraham et al., 2019).

Centralized authority also facilitates coordination across departments and functional units, enhancing preparedness through real-time collaboration and integration of specialized knowledge (AlMindeel & Martins, 2020; Buchler et al., 2018; Yoo et al., 2020; Zainudin & Nuha Abdul Molok, 2018, pp. 1–3). Effective coordination reduces information silos, accelerates the flow of threat intelligence sharing, and enables timely and coherent responses to incidents. Coordination also promotes shared accountability: when staff understand the interdependencies of their roles, they are more vigilant, communicative, and proactive in mitigation efforts (Yoo et al., 2020).

Sectoral context can impact cybersecurity preparedness by dictating the threat landscape and regulatory environment. Organizations in high-risk sectors—such as healthcare, finance, and critical infrastructure—face more frequent and sophisticated attacks due to the value and sensitivity of their data (Ignatovski, 2023; White et al., 2022). These pressures, along with stricter regulations and reputational risks, drive greater investment in advanced security and incident response protocols (Bongiovanni et al., 2022). In contrast, lower-risk sectors often face fewer cyber threats and thereby invest less, resulting in weaker preparedness.

Organizational size influences preparedness by affecting both capacity and complexity. Larger organizations possess greater resources but must manage more extensive digital infrastructures and face higher levels of threat exposure. Larger size can also lead to fragmented accountability and slower decision making, introducing vulnerabilities that offset advantages of increased resource capacity (Abraham et al., 2019; Hawdon et al., 2023). Thus, while greater size may enhance capacity to invest, it also complicates governance and coordination.

Together, these organizational factors collectively determine how cybersecurity priorities are set, resources deployed, and protective practices executed throughout the organization. When effectively aligned, they translate strategic intent into coordinated action, creating a proactive and resilient cybersecurity posture. Table D.3 in Appendix D summarizes the organizational factors impacting cybersecurity preparedness.

4.1.3. *Environmental factors*

Environmental factors encompass the external conditions that influence how organizations develop and maintain cybersecurity preparedness. These factors shape the context in which preparedness strategies are formulated, resourced, and implemented. Our thematic analysis identified five core environmental dimensions: (1) national economic capacity, (2) legal and regulatory infrastructure, (3) information-sharing ecosystems, (4) national culture, and (5) political context.

First, national economic capacity underpins both the availability of resources for cybersecurity preparedness. Stronger economies can invest more in advanced digital infrastructure and educational systems, enhancing organizations' technological capacities and expanding the pool of skilled cybersecurity professionals, thus helping to alleviate cybersecurity workforce shortages (Acheampong et al., 2024; Lee & Kim, 2020). In contrast, weaker economies often face budget constraints, outdated infrastructure, and limited access to qualified personnel, which directly impedes the ability of organizations in these countries to develop and maintain cybersecurity preparedness.

Second, legal frameworks, regulatory restrictions, industry standards, and national strategies serve as major drivers of cybersecurity preparedness (Al-ma'aitah, 2022; Mishra et al., 2022; Ovchinnikova & Upadhyay, 2023; Younies & Al-Tawil, 2020; Yudhiyati et al., 2021). These frameworks establish minimum requirements for practices such as incident reporting, data protection, and risk assessment. They exert their impact through two main mechanisms: enforcement and incentivization (Badi & Nasaj, 2023; Hasan et al., 2021; Hasani et al., 2023). Enforcement includes legal liabilities and fines for noncompliance, compelling organizations to prioritize cybersecurity to meet minimum standards to avoid regulatory sanctions. In contrast, incentives, such as tax credits or subsidies, help offset the costs of compliance, making compliance financially feasible (Li & Liao, 2018). Government-led strategies—including public awareness campaigns and capacity-building—complement enforcement and incentive mechanisms by strengthening the informational and institutional infrastructure for preparedness and by standardizing expectations across sectors (Kemp, 2023).

However, for regulations to be effective, governments must demonstrate a consistent and credible commitment to acting in the public interest on cybersecurity issues. When regulators are perceived as legitimate and competent, organizations are more likely to comply, viewing regulations as aligned with collective security goals (Skierka, 2023). In contrast, in politically volatile or mistrustful environments, regulations may be seen as tools of surveillance or control, leading to skepticism and reduced compliance (Hassib & Shires, 2021).

Regulatory effectiveness also depends on the clarity and coherence of laws. Overly complex or inconsistent regulations create ambiguity that hinders effective implementation (Abraham et al., 2019; Ardo et al., 2023; Chidukwani et al., 2024; Mishra et al., 2022), especially in decentralized systems where fragmented oversight can lead to regulatory variation and discrepancies in enforcement, resulting in delayed actions (Clark et al., 2018; Lewallen, 2021). Additionally, the global nature of cyber threats exposes the limitations of domestic regulations. Disparate national laws, inconsistent enforcement, and fragmented priorities can inhibit timely and coordinated responses to cross-border incidents, particularly for multinational organizations (Kamara, 2024). Without harmonized international standards, organizations face regulatory uncertainty, duplicative requirements, and gaps in protection. Developing shared standards and cooperative legal mechanisms is essential to address these issues and allow effective global threat response (Georgieva, 2020; Kamara, 2024).

Third, information-sharing ecosystems—particularly inter-organizational collaborations—directly enhance cybersecurity preparedness by facilitating the exchange of threat intelligence, technical expertise, and defense strategies across organizational boundaries (Badi & Nasaj, 2023; Chaudhary et al., 2018; Mermoud et al., 2019; Piazza et al., 2023; Zainudin & Nuha Abdul Molok, 2018, pp. 1–3). By aggregating knowledge across organizations, these networks expand access to threat indicators, mitigation techniques, and attack trends, thereby improving risk detection and response. Mutual accountability within these networks further motivates organizations to maintain strong practices. One form of information sharing that is impactful is public-private, as it combines regulatory leverage of the public sector with technological innovation of the private sector (Bossong & Wagner, 2017; Dong et al., 2024). The effectiveness of information-sharing initiatives depends on enabling conditions—such as trust, reciprocity, low participation barriers, and shared objectives (Mermoud et al., 2019)—and their ability to transform isolated knowledge into collective defense.

Fourth, national culture shapes both organizational strategies and individual behaviors related to cybersecurity. Cultural norms influence how risk is perceived, authority is respected, and whether best practices are socially encouraged (Shah et al., 2023). In risk-averse cultures, organizations tend to enforce stricter protocols and emphasize compliance, leading to stronger institutional safeguards. Conversely, risk-tolerant societies may display more relaxed attitudes, resulting in weaker cybersecurity practices. National culture also affects individual-level risk acceptance; where digital privacy is undervalued or rule-bending is normalized, adherence to protocols may suffer. Additionally, in rapidly digitizing countries, cultural norms regarding cybersecurity may lag behind technological change, creating vulnerabilities until social learning catches up through digital maturity (Alhalafi & Veeraraghavan, 2022).

Fifth, political context influences organizational cybersecurity preparedness by influencing both exposure to threats and institutional response capacity. In politically unstable or adversarial environments, organizations face higher risks from state-sponsored attacks, hacktivism, and digital surveillance due to heightened political tensions (Caldarulo et al., 2022; Hassib & Shires, 2021). This elevated risk prompts organizations to strengthen defenses and adopt more proactive measures (Hasani et al., 2023; Makridis & Smeets, 2019). Political volatility thus acts as both a threat multiplier and a catalyst for defensive innovation.

Collectively, environmental factors form the external landscape within which organizational cybersecurity preparedness is conceived, developed, and sustained. They determine the feasibility and urgency of protective actions by shaping the economic, legal, cultural, and political environments in which organizations operate. Table D.4 in Appendix D summarizes the environmental factors affecting cybersecurity preparedness.

4.2. Interactions between factors within domains

Determinants of cybersecurity preparedness operate not only as standalone drivers but also interact within domains. These intra-domain interactions can reinforce, amplify, or in some cases moderate the overall effect of individual factors on preparedness. Understanding these internal dynamics is essential, as readiness often emerges from the combined influence of interrelated factors within a domain, rather than from isolated inputs. Systematically examining these intra-domain synergies and tensions is therefore key to capturing a more complete picture of how cybersecurity capacity is built and maintained. The findings in this section responds to the second part of RQ1 on how factors interact to shape preparedness, by identifying and analyzing empirical evidence on interactions within each non-technological domain.

4.2.1. Interactions among human factors

Within the human dimension, cybersecurity research has increasingly explored how individual-level factors interact through mediating and moderating mechanisms. Psychological stress can weaken an individual's ability to absorb information during training and affect subsequent cybersecurity behaviors. Here, psychological stress may function as a moderator: high stress levels can reduce the effectiveness of training by impairing attention, memory retention, or decision-making, thus weakening the relationship between training and secure behavior (Hong et al., 2023). This highlights that preparedness depends not only on knowledge acquisition, but also on individuals' psychological readiness.

Proposition 1. *The positive effect of cybersecurity training on secure behavior is weakened when psychological stress among employees is high.*

Training would also be more effective if tailored to generational differences of employees as learning preferences, technological familiarity, and communication styles can vary significantly across age groups (Li et al., 2022).

Proposition 2. *The positive effect of cybersecurity training on secure behavior is stronger when tailored to generational differences.*

Empirical evidence also suggests that training and cybersecurity self-efficacy are mutually reinforcing. Employees with higher initial self-efficacy learn more from training interventions, while successful training experiences further boost their perceived capability, increasing long-term engagement and compliance (Hasani et al., 2023; Smith et al., 2021)

Proposition 3. *Cybersecurity training and individual self-efficacy interact synergistically, such that higher self-efficacy enhances training outcomes, and effective training further increases self-efficacy, resulting in greater long-term compliance.*

Emotions such as fear interact with prior experience to influence how urgently and seriously individuals respond to cybersecurity threats. For instance, employees with prior experience of a cyber incident are more responsive to fear-based messaging, suggesting that prior experience enhances emotional salience and compliance behavior (Ng et al., 2021; Schuetz et al., 2020).

Proposition 4. *The effectiveness of fear-based cybersecurity messaging is amplified for employees with prior experience of cyber incidents, resulting in greater urgency and compliance.*

In sum, human factors interact in complex, and often synergistic ways to promote preparedness. While research highlights the value of integrating cognitive, emotional, and experiential dimensions to improve preparedness, few studies examine their interactions across diverse contexts. Developing integrative frameworks to capture these interactions, within varied sectoral and organizational settings, remains a critical step for advancing cybersecurity readiness.

4.2.2. Interactions among organizational factors

Within the organizational domain, multiple internal factors interact to influence cybersecurity preparedness, often as mediators or moderators. First, leadership's influence on employee security behavior is typically mediated by organizational culture, where strong leadership improves compliance primarily by creating supportive cultural norms (Onumo et al., 2021), indicating that leadership's impact is channeled through the organization's cultural norms.

Proposition 5. *The effect of organizational leadership on cybersecurity compliance is mediated by the strength of the organization's cybersecurity culture.*

Other research finds that top management support *moderates the impact of organizational cybersecurity policies and strategies, strengthening their effect when management visibly endorses these efforts* (Hasan et al., 2021). *Executive* support *signals priority, reinforces compliance, and helps embed formal policies into everyday organizational behavior.*

Proposition 6. *The positive relationship between organizational cybersecurity policies and compliance is strengthened when top management provides visible and active support.*

Organizational structure also influences how coordination and planning reinforce each other. Centralized governance improves intra-organizational coordination by reducing redundancy and promoting consistent implementation of policies across departments (Auffret et al., 2017; Caldarulo et al., 2022). *This structural clarity strengthens communication, facilitates strategy execution, and enables unified responses to threats.*

Proposition 7. *Centralized governance structures amplify the positive effects of coordination and planning on cybersecurity preparedness by reducing operational fragmentation and promoting consistent implementation.*

Cybersecurity investment strategy also interacts with governance structure. Centrally coordinated investments can achieve greater cost-effectiveness through spillover effects, amplifying the impact of each dollar spent (Armenia et al., 2019). *In contrast, decentralized organizations may face resource duplication, inconsistent implementation, and siloed decision-making—diminishing the effectiveness of even substantial cybersecurity investments.*

Proposition 8. *Centrally coordinated cybersecurity investments yield higher preparedness outcomes compared to decentralized investment approaches, due to improved cost-effectiveness and reduced resource duplication.*

Taken together, the interplay among organizational factors is well-documented in the literature. Their combined effects shape the organizational environment through cascading and reinforcing pathways. However, many of these interactions remain empirically underexplored, highlighting the need for further research.

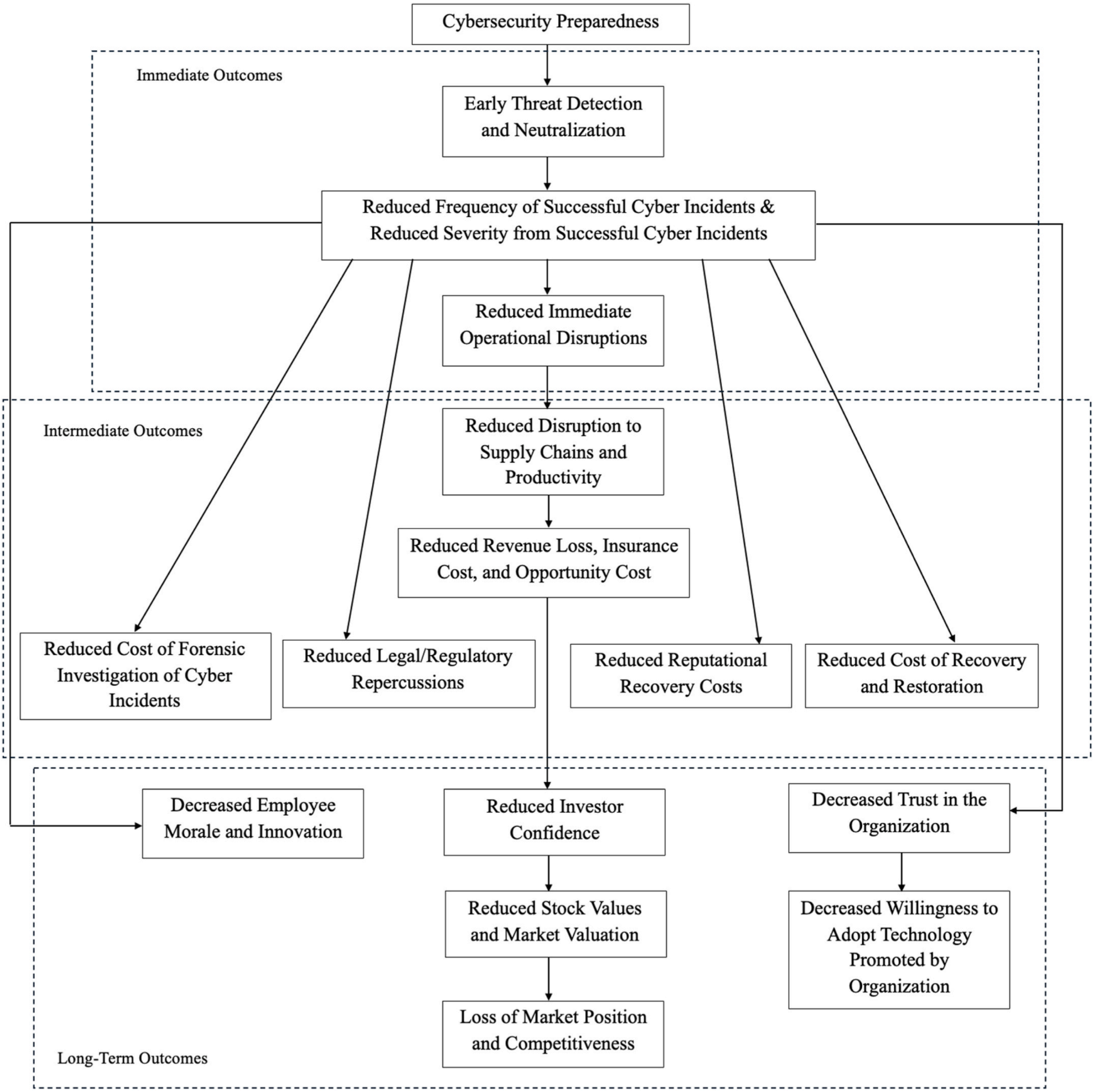
Cybersecurity Preparedness
Immediate Outcomes
Early Threat Detection and Neutralization
Reduced Frequency of Successful Cyber Incidents & Reduced Severity from Successful Cyber Incidents
Reduced Immediate Operational Disruptions
Intermediate Outcomes
Reduced Disruption to Supply Chains and Productivity
Reduced Revenue Loss, Insurance Cost, and Opportunity Cost
Reduced Cost of Forensic Investigation of Cyber Incidents
Reduced Legal/Regulatory Repercussions
Reduced Reputational Recovery Costs
Reduced Cost of Recovery and Restoration
Decreased Employee Morale and Innovation
Reduced Investor Confidence
Decreased Trust in the Organization
Reduced Stock Values and Market Valuation
Decreased Willingness to Adopt Technology Promoted by Organization
Loss of Market Position and Competitiveness
Long-Term Outcomes

Fig. 4. Outcomes of cybersecurity preparedness categorized by time horizons.

4.2.3. Interactions among environmental factors

The interplay between environmental factors is the least studied of all categories and remains largely speculative in the literature. Environmental determinants of cybersecurity are typically examined in isolation, and, to our knowledge, no empirical studies to date have tested how multiple environmental factors interact to influence cybersecurity preparedness. For example, it is unclear whether a stringent regulatory regime can offset risks posed by a hostile threat landscape, or whether strong market competition combined with legal pressure yields multiplicative effects on organizations' security investments.

Proposition 9. *Stringent regulatory regimes are more effective in promoting organizational cybersecurity preparedness when external cyber threats are severe, as strong regulations can offset the risks from hostile threat environments.*

The interplay between environmental factors thus remains an open research frontier, with very limited empirical evidence available.

4.3. Interactions between factors across domains

Researchers have increasingly examined how determinants from different domains interact to shape cybersecurity preparedness. Cross-domain interactions cut across categories, linking internal organizational structure and actions to shifts in cybersecurity-related behavioral dynamics. Understanding these dynamics is critical for developing integrated strategies that ensure interventions in one domain are compatible with capacities and constraints in others. The findings in this section address the second part of RQ1 by showing how cross-domain interactions among human, organizational, technological, and environmental factors collectively shape cybersecurity preparedness.

4.3.1. Human and organizational interactions

Organizational policies and culture strongly influence individual cybersecurity behaviors. A strong cybersecurity culture promotes organizational commitment to ongoing, high-quality training and communication (Li et al., 2022). Organizational training and communications improve cybersecurity readiness through mechanisms mediated by individual-level factors, such as improved awareness, knowledge, and vigilance to threats. Moreover, supportive leadership strengthens compliance with security protocols by fostering a sense of personal responsibility among staff, increasing adherence to cybersecurity policies (Solomon & Brown, 2021).

Human factors may also moderate the effectiveness of organizational training and communication efforts. Employees with higher cybersecurity knowledge and motivation are more receptive to training and more capable of applying security protocols in practice (Solomon & Brown, 2021). This suggests that individual readiness can moderate how well organizational initiatives translate into behavior change. Empirical studies consistently show that combining human-centric initiatives (e.g., skills training, awareness campaigns) with organizational commitment (e.g., engaged leadership, policy enforcement) yields significantly better preparedness outcomes than either approach alone.

Proposition 10. *The effectiveness of organizational cybersecurity policies and training on employee compliance is amplified when employees possess high levels of cybersecurity awareness and motivation.*

4.3.2. Human and technological interactions

While the adoption of advanced cybersecurity tools is often expected to enhance an organization's protection, their effectiveness depends on users' technological competency and security awareness (Lee & Kim, 2020). Without sufficient user technical expertise, sophisticated cybersecurity tools may be misconfigured or misused, potentially leading to greater vulnerabilities or a false sense of security. Overreliance on poorly understood tools without an understanding of their limitations may actually decrease vigilance and increase risky behaviors. Secure practices are most likely when positive cybersecurity attitudes are paired with accessible and supportive technologies (Onumo et al., 2021). Thus, preparedness requires not only investments in technological infrastructure, but also ongoing capacity-building through personnel training and the promotion of positive cybersecurity attitudes. No single component is sufficient on its own; their integration is essential for achieving lasting readiness.

Proposition 11. *The impact of advanced cybersecurity technologies on organizational preparedness is maximized when end-users have high levels of technological competence, security awareness, and positive cybersecurity attitudes.*

4.3.3. Organizational and technological interactions

Organizational leadership is a mediating factor in shaping cybersecurity preparedness, particularly through its influence on security technology adoption and use (Hasani et al., 2023). Leadership that actively prioritizes cybersecurity is associated with greater uptake of security technologies, which in turn enhances preparedness. Moreover, leadership also moderates the effectiveness of technological implementation. Without visible and sustained support from leadership, even the most sophisticated systems may be underutilized, poorly maintained, or inadequately integrated into daily operations (Berlilana et al., 2021).

Further, advanced cybersecurity technologies are only effective when supported by strong organizational governance. Without formal policies, clear procedures, and resource commitments, staff lack the guidance and capacity to use cybersecurity tools appropriately, limiting the impact of technology (Chidukwani et al., 2024). In contrast, robust governance frameworks and risk-informed strategies ensure technologies are well-integrated to operations and effectively utilized (Berliliana, 2021; Srivastava et al., 2020).

Proposition 12. *The relationship between technological adoption and cybersecurity preparedness is strengthened by clear governance frameworks and engaged leadership, which ensure technologies are effectively integrated and utilized.*

4.4. Consequences of cybersecurity preparedness

Cybersecurity preparedness generates a range of organizational outcomes that unfold across different time horizons: immediate, intermediate, and long-term. The findings from this section respond to RQ2 regarding the outcomes of preparedness across different time horizons. Fig. 4 visually synthesizes the immediate, intermediate, and long-term organizational outcomes of cybersecurity preparedness extracted from this literature review. It illustrates how these outcomes build upon one another, showing that failure to address early vulnerabilities can lead to more severe consequences, whereas strong preparedness can produce compounding benefits over time. In addition to identifying these outcomes, we examine the mechanisms through which cybersecurity preparedness influences outcomes. By doing so, we highlight not only what changes as a result of preparedness, but also how these changes occur—shedding light on the processes that connect preparedness to various temporal impacts.

4.4.1. Immediate outcomes

First, cybersecurity preparedness directly reduces an organization's vulnerability to cyber threats by decreasing the frequency, severity, and success rate of cyberattacks (Hasan et al., 2021; Srivastava et al., 2020; Tsen et al., 2022). Prepared organizations are better equipped to detect and neutralize threats early, limiting incidents such as phishing attacks, ransomware, malware, and denial-of-service incidents (Dinkova et al., 2023; Dutton et al., 2019; Kalogiannidis et al., 2023; Kandasamy et al., 2022; Pienta et al., 2020).

Second, in cases where attacks do succeed, organizations with low preparedness often suffer severe operational disruptions and breaches of sensitive assets. Incidents may involve theft or compromise of intellectual property, financial records, customer data, and patient information (Khan et al., 2021; Lis & Mendel, 2019). Cyberattacks can also result in alteration, deletion, or blocked access to critical digital assets, resulting in system outages and service interruptions (Khan et al., 2021; Lis & Mendel, 2019; Tsen et al., 2022).

4.4.2. Intermediate outcomes

In the intermediate term, successful breaches from cyberattacks impair both public and private sector operations by disrupting supply chains, interrupting utility delivery, reducing productivity, and damaging institutional reliability (Khan et al., 2021; Lis & Mendel, 2019; Tsen et al., 2022).

Beyond operational disruptions, organizations also face financial and legal consequences. These include direct costs such as forensic investigations, data recovery, system restoration, and required notification of affected parties (Lis & Mendel, 2019; Meisner, 2018; von Skarczinski, Dreißigacker, & Teuteberg, 2022). Organizations may also face increased operational costs from public-relations efforts aimed at restoring their brand image and public confidence (Meisner, 2018; Romanosky, 2016). Indirect costs often follow, including lost revenue, increased insurance premiums, and opportunity costs due to downtime and resource diversion during recovery (Hawdon et al., 2023; von Skarczinski et al., 2022). Legal repercussions may also emerge in the form of regulatory fines and lawsuits, particularly in high-profile breaches, especially where negligence is perceived (Hawdon et al., 2023; Khan et al., 2021; Meisner, 2018; Romanosky, 2016).

These intermediate financial and legal burdens can be partially mitigated when organizations publicly disclose cybersecurity practices and demonstrate compliance with industry standards, actions that enhance stakeholder trust and reduce reputational damage (Al Amosh & Khatib, 2025; Frank et al., 2021).

4.4.3. Long-term outcomes

In the long term, poor cybersecurity preparedness can erode core organizational capacities and strategic positioning. Internally, severe breaches can degrade employee morale and increase turnover, weakening long-term productivity and impeding innovation (Tsen et al., 2022). In competitive industries, consequences may include loss of market position due to leaked intellectual property or the departure of critical personnel to rival firms (Berlilana et al., 2021; Khan et al., 2021).

Reputational damage represents another enduring consequence. Cyber incidents can erode customer trust, damage brand image, and decrease willingness to adopt digital services, especially in sectors reliant on personal data, such as healthcare and finance. Persistent negative perceptions of an organization's cybersecurity preparedness can deter public adoption of new digital technologies, ultimately compromising service delivery and customer experience personalization efforts. Over time, this can raise operational costs while further diminishing organizational revenue, profits, stock values, and market valuation (Abdelhamid et al., 2019; Alharbi et al., 2017; Berlilana et al., 2021; Hawdon et al., 2023).

These reputational effects can also have sustained impacts on investor confidence, especially for private firms, where perceived risk carries significant weight (Juma'h & Alnsour, 2021; Smith et al., 2023). Over the long term, diminished trust can lead to reduced capital access and heightened scrutiny from stakeholders. While proactive disclosure of cybersecurity risk mitigation strategies can gradually restore investor trust and confidence, reputational recovery is often slow and uneven (Huang & Murthy, 2024). The severity and duration of reputational harm are shaped by the type and magnitude of the breach, with more severe and prolonged incidents extending negative perceptions (Juma'h & Alnsour, 2021). Nonetheless, strong leadership and a swift, transparent organizational response can mitigate these effects and help restore public confidence over time, highlighting the role of organizational governance in moderating long-term reputational trajectories.

Table E.1 in Appendix E summarizes the consequences of cybersecurity preparedness. In sum, cybersecurity preparedness is associated with a continuum of positive outcomes, including reduced vulnerability to attack, minimized operational and financial losses, and improved reputational resilience. When organizations develop assessment frameworks and plan their cyber defenses, they should account not only for the immediate outcomes of preparedness but also for its intermediate and long-term impacts.

5. Discussion and future research agenda

Recent research has greatly expanded our understanding of organizational cybersecurity preparedness, particularly regarding its determinants and consequences. Nevertheless, several important gaps remain, many of which directly relate to the propositions developed in this study.

First, while this review has proposed that intra-domain and cross-domain interactions—such as those among human factors, or between organizational leadership and culture—are critical to cybersecurity readiness, current research seldom includes these interactions in assessment frameworks or systematically tests these relationships, and theoretical development on interactions remains limited in some domains. Future studies and frameworks should move beyond isolated factor analysis to identify, empirically test, and incorporate comprehensive interactions. For example, studies should examine how combinations of human factors like self-efficacy, training, and emotional states interact to influence both individual cybersecurity behavior and overall organizational preparedness. Additionally, research should investigate how organizational leadership and culture jointly mediate or moderate the effectiveness of cybersecurity interventions. Comparative, multi-factor studies—ideally using experimental or longitudinal designs—are needed to validate and refine these interaction-based propositions.

Second, our results suggest that the effectiveness of investments in one domain, such as technology or training, may only be effective when reinforced by complementary factors, including organizational structure, culture, or individual motivation. To address this, future research should assess the relative and combined impacts of different types of investments. This includes comparing the returns on investment of technical versus human- or organization-focused cybersecurity interventions, and to analyze how these returns change when moderators are present or absent. Such analyses will help organizations prioritize interventions that offer the greatest impact under specific conditions.

Third, several propositions point to the importance of context—such as organizational size, sector, national legal environment, and cultural norms—in shaping preparedness. However, few existing frameworks adequately account for these contextual effects. Future research should test whether the propositions about sectoral and environmental influences hold across diverse organizational settings and develop context-sensitive assessment tools. For example, scholars could examine how the effectiveness of preparedness strategies varies by organizational context, or how differences in national data protection laws influence the adoption and enforcement of cybersecurity practices across different sectors and jurisdictions.

Fourth, this review highlights dynamic interactions, such as how the influence of leadership or regulatory pressure may change over time or in response to cyber incidents. Longitudinal research is necessary to test propositions about the evolving effects of these factors and their interactions, as well as to understand the time-dependent trajectories of organizational cybersecurity readiness and recovery after incidents. Relevant questions include how the relationships between leadership, organizational culture, and preparedness evolve in response to emerging threats and in the aftermath of cyber incidents, as well as what lasting impacts regulatory interventions have on organizational cybersecurity behavior and outcomes.

Finally, as the adoption of artificial intelligence (AI) grows, new propositions emerge regarding the interplay between human expertise and AI-enabled cybersecurity solutions, as well as the risks posed by AI-driven attacks. Future research should empirically examine whether robust human-AI integration improves preparedness and identify organizational and human factors that support the effective integration of AI tools for cybersecurity. Particular attention should be given to the dual role of AI, both as a defensive tool and a source of threats. This includes examining agentic AI systems capable of autonomous decision-making, which may transform both defensive strategies and the nature of cyber threats. Understanding how AI-enabled defenses and AI-driven attacks interact to shape organizational resilience, and what training is needed to optimize this balance, is an essential frontier for evolving cybersecurity preparedness frameworks in an increasingly AI-centric era.

In summary, the propositions articulated in this review regarding intra- and cross-domain interactions, mediating and moderating mechanisms, contextual variation, longitudinal dynamics, and the integration of emerging technologies offer a roadmap for future empirical studies. Testing and refining these propositions and addressing the research questions outlined above will support the development of more robust, adaptable, and evidence-based models of cybersecurity preparedness in an ever-evolving threat landscape.

6. Conclusion

This systematic literature review set out to synthesize and critically analyze research on cybersecurity preparedness, reviewing 129 articles published between 2016 and 2024. Current cybersecurity preparedness assessment frameworks often prioritize technological components, at the expense of equally important human, organizational, and environmental factors. Moreover, these frameworks seldom fully address the complex interrelationships among various determinants of preparedness and the multifaceted outcomes that follow. To address this gap, our review systematically and comprehensively identified three broad categories of non-technological factors—human, organizational, and environmental—that not only contribute to cybersecurity preparedness but also interact with one another to influence preparedness. Furthermore, this review examined the outcomes of cybersecurity preparedness, revealing its crucial role not only in mitigating immediate threats but also in supporting the long-term sustainability and strategic success of organizations.

6.1. Theoretical and practical implications

Theoretically, this review advances the field of cybersecurity preparedness by broadening the conceptualization of preparedness beyond narrow technological dimensions. By integrating findings from diverse empirical traditions, this study unifies previously fragmented research and enhances coherence around the determinants of preparedness—especially through the articulation of a more comprehensive set of non-technological factors and the analysis of interactions both within and across domains. In doing so, it underscores the need to view cybersecurity preparedness as a dynamic, multi-domain construct, shaped by intersecting influences, rather than as a static or purely technological condition. Additionally, the review draws attention to the fact that the consequences of cybersecurity preparedness are not always immediate or directly observable. Some impacts only unfold over extended time horizons, and their manifestation may depend on a complex interplay of internal and external factors. Recognizing these delayed and indirect effects is essential for building more realistic and nuanced models of cybersecurity impact, thereby promoting systems-oriented approaches in future research.

Practically, this review addresses a pressing need among decision-makers and practitioners. By distilling lessons from diverse empirical studies, it provides actionable guidance for developing strategic interventions and assessment frameworks that account for the interplay of technological, human, organizational, and environmental dimensions. A comprehensive understanding of both direct and indirect consequences also equips organizations to better anticipate risks, plan proactively, and assess the broader impact of their cybersecurity investments. This integrated perspective enables organizations to align cybersecurity strategies with specific operational realities, resource constraints, and evolving threat environments. To our knowledge, this is among the first systematic reviews to map the full range of non-technological factors and their cross-domain interactions, while also synthesizing both short- and long-term organizational impacts.

6.2. Limitations of this research

Despite its contributions, this review has certain methodological limitations. Most notably, the literature search was restricted to select academic databases and to English-language publications, thus excluding non-English works and potentially relevant government or industry reports. These exclusions may result in overlooked perspectives or findings that could further inform our understanding of cybersecurity preparedness. Future research should seek to broaden the scope of literature, potentially incorporating real-time data, grey literature, and sources from multiple languages to enrich and validate the insights presented here.

Second, while the manual approach to literature identification and coding allows for interpretive depth, it limits scalability and replicability. Future reviews could enhance breadth and analytical rigor by integrating machine learning tools (particularly Natural Language Processing tools) to automate study selection, thematic analysis, and pattern recognition. This offers a promising methodological direction for continuous and systematic synthesis in the ever-evolving field of cybersecurity preparedness.

Moreover, while this article discusses the determinants and consequences of cybersecurity preparedness in general terms, it does not provide sector-specific models. Given the variation in cybersecurity risks, threats, and contexts across industries—such as healthcare, critical infrastructure, and others—there is a clear need for tailored, sector-specific assessment tools. This review should therefore be viewed as a guiding framework to inform the development of more customized models that address the unique challenges of individual sectors.

CRediT authorship contribution statement

Songkhun Nillasithanukroh: Writing – review & editing, Writing – original draft, Methodology, Formal analysis, Data curation, Conceptualization. **Chul Hyun Park:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Methodology, Formal analysis, Data curation, Conceptualization. **Jaejong Baek:** Writing – review & editing, Conceptualization. **Gail-Joon Ahn:** Writing – review & editing, Conceptualization. **Robert Richards:** Writing – review & editing, Conceptualization.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendices.

Appendix APICO Framework Utilized

Table A.1
Search Term Development Based on PICO Framework

PICO Component	Definition in This Review	Example Keywords
Population (P)	Organizations of any type (public, private, nonprofit) involved connected digitally, making them vulnerable to cybersecurity threats	"organization*" OR "enterprise*" OR "institution*" OR "business*" OR "firm*" OR "agency"
Intervention (I)	Cybersecurity preparedness efforts, including contributing factors and mechanisms. Contributing factors encompass technological and especially non-technological determinants. Mechanisms refer to the processes or pathways through which these inputs influence preparedness.	"cybersecurity preparedness" OR "cyber readiness" OR "cyber resilience OR "information security preparedness" AND ("factor*" OR "driver*" OR "influenc*" OR "mechanism*" OR "process*" OR "moderator*" OR "mediator*")
Comparison (C)	Review focuses on synthesis of findings across studies, not comparative groups.	N/A
Outcome (O)	Outcomes or consequences of cybersecurity preparedness (e.g., risk reduction, incident response effectiveness)	"outcome*" OR "impact*" OR "effect*" OR "result*" OR "consequence*" OR "risk mitigation" OR "resilience" OR "performance"

Appendix B. Metadata Collected from Articles Included in the Systematic Literature Review

Table B.1
Overview of Metadata Information Collected from the Included Articles

Category	Metadata	Description
Descriptive information	Article title	The title of the article.
	Author(s)	The name of the article's author(s).
	Source Title	The title of the journal or conference proceedings that the article is from.
	Keywords	Keywords that the author(s) provided for the article.
	Database found through	The database that was used to find the article.
	Publication year	The year that the article was published.
	Digital Object Identifier (DOI) or website	The DOI of the study when available. If not available, the website in which the study can be found.
	Abstract	The abstract of the article.
Content-related information	Type of factors	The type of factors contributing to cybersecurity preparedness under study. (e.g. technological, human, organizational, environmental)
	Specific factors	Details the specific factors that each study proposes to influence cybersecurity preparedness.
	Framework or standards	The framework or standard used to assess the cybersecurity preparedness or vulnerability to risks as well as the components of the framework or standard.
	Impacts and consequences	The impacts and consequences of cybersecurity preparedness or lack thereof.

Appendix C. Full List of Literature Included in Data Extraction and Thematic Analysis

The complete list of the literature reviewed in the systematic literature review, categorized by topics (technological factors, human factors, organizational factors, environmental factors, intra-domain interactions, inter-domain interactions, and consequences), is provided in the document linked here:

https://docs.google.com/spreadsheets/d/1DMsZVpApSaH-mvCWeWxqhT6E9EpZpXg7lofO_0XHgL8/edit?usp=sharing.

Appendix D. Summary of Technological, Human, Organizational, and Environmental Factors Influencing Cybersecurity Preparedness

Table D.1
Summary of Technological Factors Influencing Cybersecurity Preparedness

Category	Factor	References
Cybersecurity hardware	Availability of hardware	Hasan et al., 2021; Malatji et al., 2019, 2020; Berlilana et al., 2021; Neri et al., 2024
Cybersecurity software	Availability of software	Hasan et al., 2021; Malatji et al., 2019, 2020; Berlilana et al., 2021; Neri et al., 2024; Shah et al., 2023
	Update of software	Kioskli et al. (2023)
Network systems	Well-designed network that can limit the spread of attack	Yeoh et al., 2023; Shah et al., 2023
	Centralized access management for the network	Alruwies et al., 2022
Automation tools	Utilization of AI and machine learning to address cyber threats	Falco et al., 2018; Canham et al., 2021; Bokhari & Myeong, 2023; Biswas, Mukhopadhyay, Bhattacharjee, Kumar, & Delen, 2022

(continued on next page)

Table D.1 (*continued*)

Category	Factor	References
	Blockchain technology to improve security of transactions	Abd El-Latif et al. (2021)
Backup system	Existence of a backup system	Chapman and Reithel (2021)
Digital forensics	Capacity to conduct digital forensics to investigate cyberattacks	Ariffin & Ahmad, 2021; Tsado et al., 2024
Dependence on technology and IT utilization	Level of dependence on technology and IT utilization	Srivastava et al., 2020; Frandell & Feeney, 2022; Arroyabe et al., 2024
	Controlling number of and monitoring access points and attack surface	Caldarulo et al. (2022)
	Managing and monitoring of internal network connectivity	Borenius et al. (2022)
External connectivity	Cybersecurity preparedness of external organizations	Badi and Nasaj (2023)
	Monitoring of externally connected IT channels	Borenius et al. (2022)

Table D.2
Summary of Human Factors Influencing Cybersecurity Preparedness

Category	Factor	References
Knowledge	Cybersecurity knowledge and cybersecurity awareness of IT personnel and organization's employees	Althobaiti, 2021; Ani et al., 2019; Alhalafi & Veeraraghavan, 2022; Chapman & Reithel, 2021; Abd Rahim et al., 2019
	Uniform level of cybersecurity knowledge across all members of the organization	Ani et al., 2019
Training	Availability of cybersecurity skill training provided to IT personnel and organization's employees	Sapanca & Kanbul, 2022; Kioskli et al., 2023; Berlilana et al., 2021; Badi & Nasaj, 2023
	Availability of general IT skill training received by IT personnel and organization's employees	AlMindeel & Martins, 2020;
	Breadth of knowledge covered in a training	Canham et al., 2021; Armstrong et al., 2020; Chapman & Reithel, 2021; Abd Rahim et al., 2019
	User-friendly training program	Kam et al., 2022; AlMindeel & Martins, 2020
	Regular and mandatory training	Hasan et al., 2021; AlMindeel & Martins, 2020
Past experiences	Past experiences with cyber incidents	Smith et al., 2021; Nam, 2019; Chapman & Reithel, 2021; Li et al., 2019; Fusi et al., 2023
	Characteristics of past experiences with cyber incidents	Kostyuk & Wayne, 2021
	Experiences in IT roles	Smith et al., 2021
Cognitive capacity of organizational members	Mental fatigue from overburdening employees with cybersecurity policies and programs	Smith et al., 2021; Kim & Kim, 2024
Intrinsic factors	Positive attitude toward cybersecurity	Onumo et al., 2021; Vafaei-Zadeh et al., 2019
	Intrinsic motivation to reduce risky online behavior	Neigel et al., 2020
	Personality traits	Li et al., 2023
	Personal calculations of cost and benefit	Yudhiyati et al., 2021
	Strong sense of responsibility	Posey & Folger, 2020; AlMindeel & Martins, 2020
	Value alignment	Hasan et al., 2021
	Trust in society and of the cyber world	Wong et al., 2022; Nam, 2019
Emotions	Feeling of fear	Schuetz et al., 2020; Ng et al., 2021
Demographic factors	Age	Neigel et al., 2020; Li et al., 2023; Lee & Kim, 2020
	Gender	Sapanca & Kanbul, 2022; Neigel et al., 2020; Anwar et al., 2017
	Educational background	Allodi et al., 2020
Incentive schemes	Existence of rewards and penalties scheme	AlMindeel & Martins, 2020
	Size of rewards	Chen et al., 2021

Table D.3
Summary of Organizational Factors Influencing Cybersecurity Preparedness

Category	Factor	References
Organizational leadership	Awareness and support of cybersecurity	Onumo et al., 2021; Abraham et al., 2019; Al-ma'aitah, 2022; Auffret et al., 2017; Hasan et al., 2021
	Allocation of resources for cybersecurity	Al-Kumaim & Alshamsi, 2023
	Enforcing cybersecurity politics	Al-Kumaim & Alshamsi, 2023
	Support for social media and open data initiatives	Frandell & Feeney, 2022
Organizational culture	Existence of positive cybersecurity culture	Onumo et al., 2021; Li et al., 2019; Dong et al., 2024; Hasan et al., 2021; Kessler et al., 2020
	Culture of cybersecurity knowledge sharing and collaboration	AlMindeel & Martins, 2020
	Culture that views humans as a part of solution rather than a part of problem	Zimmermann & Renaud, 2019
Investments in cybersecurity	Level of investments in cybersecurity	Dinkova et al., 2023; Berlilana et al., 2021; Yudhiyati et al., 2021; White et al., 2022; Hasan et al., 2021; Auffret et al., 2017; Fusi et al., 2023
	Optimization plan for cybersecurity investments	Kissoon, 2020; Armenia et al., 2019

(*continued on next page*)

Table D.3 (*continued*)

Category	Factor	References
Organization's technology department	Centralized technology department	Caldarulo et al., 2022
	Presence of a chief information security officer	Auffret et al., 2017
Cybersecurity strategic plan	Existence of an up-to-date cybersecurity strategic plan	He et al., 2022; Chowdhury et al., 2023; Pollini et al., 2022
	Adaptive policy design	Porter & Tan, 2023
	Inclusion of cybersecurity performance evaluations in the plan	Hochstetter-Diez et al., 2023; Chandra et al., 2022; Hasan et al., 2021; AlMindeel & Martins, 2020
	Awareness of cybersecurity plan among employees	Li et al., 2019
	Participation of employees in the development of cybersecurity plan	Pham et al., 2019
Organizational coordination	Capacity for members with various specializations and competencies to coordinate	Buchler et al., 2018; Yoo et al., 2020; AlMindeel & Martins, 2020
	Monitoring of others' cybersecurity behavior	Yoo et al., 2020
Characteristic of organization	Sector of operation	Ignatovski, 2023; White et al., 2022; Bongiovanni et al., 2022
	Size of organization	Hawdon et al., 2023; Abraham et al., 2019

Table D.4
Summary of Environmental Factors Influencing Cybersecurity Preparedness

Category	Factor	References
National economic resources	Size of economic resources	Lee & Kim, 2020
Legal factors and policy frameworks	Existence of cybersecurity legal framework, regulations, industry standards, and national strategy	Ovchinnikova & Upadhyay, 2023; Mishra et al., 2022; Yudhiyati et al., 2021; Al-ma'aitah, 2022; Hasan et al., 2021; Badi & Nasaj, 2023
	Fines and penalties as consequence of violation	Li & Liao, 2018
	Subsidies and tax incentives for positive cybersecurity behavior	Li & Liao, 2018
	National strategy that invests in cybersecurity	Kemp, 2023
	Regulations and laws written with the purpose of promoting cybersecurity preparedness	Hassib & Shires, 2021
	Regulatory legitimacy of government in enforcing laws	Skierka, 2023
	Complex legal framework and/or conflicts between laws and regulations	Mishra et al., 2022; Ardo et al., 2023; Abraham et al., 2019; Clark et al., 2018
	Strict enforcement of laws and regulations	Lewallen, 2021
	Existence of international laws, regulations, and standards	Georgieva, 2020
Relationship with external organizations	Information sharing agreement between partner organizations	Piazza et al., 2023; Mermoud et al., 2019; Badi & Nasaj, 2023
	Accountability-promoting partnership	Chaudhary et al., 2018
	Public-private partnership	Bossong & Wagner, 2017
Culture	Country's culture regarding cybersecurity	Shah et al., 2023; Alhalafi & Veeraraghavan, 2022
Political environment	Political uncertainty and political competition	Hassib & Shires, 2021; Caldarulo et al., 2022

Appendix E. Summary of Cybersecurity Preparedness Consequences

Table E.1
Summary of the Consequences of Cybersecurity Preparedness

Category	Consequences	References
Cyber incidents	Frequency of cyber incidents	Hasan et al., 2021
	Severity of cyber incidents	Tsen et al., 2022
	Types of cyber incidents	Pienta et al., 2020; Kandasamy et al., 2022; Kalogiannidis et al., 2023; Dutton et al., 2019; Dinkova et al., 2023
Data owned by an organization	Theft of data	Khan et al., 2021; Tsen et al., 2022; Lis & Mendel, 2019
	Alteration and deletion of data	Khan et al., 2021
	Loss of access to data	Khan et al., 2021; Lis & Mendel, 2019
Direct costs	Decline in financial performance (e.g. revenue, profits, returns)	Smith et al., 2023; Juma'h & Alnsour, 2021; Hawdon et al., 2023; Berlilana et al., 2021
	Restoring and repairing of operational system	Lis & Mendel, 2019
	Recovery of data	von Skarczinski, Dreißigacker, & Teuteberg, 2022
	Legal fines and fees	Khan et al., 2021; Hawdon et al., 2023; Meisner, 2018; Romanosky, 2016
	Forensic investigation of cyber incident	Meisner, 2018
	Cost of notifying affected customers	Meisner, 2018
	Cost of public relations to restore confidence and trust in the operation of the organization and its cybersecurity capacity	Meisner, 2018; Romanosky, 2016
Indirect costs	Reduced trust, confidence, and loyalty in firms' operations	Smith et al., 2023; Hawdon et al., 2023; Berlilana et al., 2021; Yudhiyati et al., 2021; Hasan et al., 2021; Shandler and Gomez, 2023
	Unwillingness to adopt new technologies introduced by the organization	Alharbi et al., 2017; Abdelhamid et al., 2019
	Opportunity cost	Hawdon et al., 2023; von Skarczinski et al., 2022
	Productivity loss and decreased operational efficiency	Tsen et al., 2022
	Long-term growth prospects	Tsen et al., 2022
	Decline in competitive advantage of organization	Khan et al., 2021; Berlilana et al., 2021

Appendix F. Review of Cybersecurity Assessment Framework and Approaches

Table F.1
Summary of Existing Cybersecurity Assessment Frameworks

Study	Framework/Approach	Sector/Context	Gaps/Limitations
Aliyu et al. (2020)	Maturity model informed by NIST CSF, ISO/IEC 27001, ENISA	Higher education	Limited to education; lacks broader theory testing; focus primarily on assessing technological capacity to defense against cyber threats; lacks discussion of interactions between factors; minimal integration of dynamic preparedness outcomes over time
Ahouanmenou et al. (2023)	Informed by NIST CSF, ISO	Healthcare	Emphasizes technological controls; underrepresents human and organizational factors; acks examination of cross-domain interactions and preparedness outcomes
Antunes et al. (2022)	Client-Centered Information Security Management (CCISM) Framework	SMEs	Emphasis on technical controls and audit processes; limited exploration of human/organizational dynamics; lacks theory testing or validation of cross-domain factor interactions
Delgado et al. (2021)	NIST CSF	Government organizations	Strong technical orientation; minimal incorporation of human and organizational readiness (only training); lacks analysis of factor interactions or preparedness outcomes; limited empirical testing across diverse organizational types
Bahuguna et al. (2019)	ITU's Global Cybersecurity Index	Mixed sectors	Self-reported, unverified data; lacks statistical rigor or theory testing; includes but does not deeply analyze human and organizational factors (training, management, policies, budget allocation); lacks discussion of interactions between domains or preparedness outcomes
Barraza de la Paz et al. (2023)	Informed by NIST CSF + ISO/IEC 27005 + MAGERIT	Mixed sectors	No empirical testing or original model proposed; discussion of human/organizational factors not comprehensive (human error, training and awareness, governance. culture); fragmented literature with inconsistent integration of human, organizational, and technical domains; minimal discussion of interactions between risk factors; outcomes of preparedness not assessed
Bernardo et al. (2025)	Custom evaluation framework around cybersecurity practices in industrial control systems (ICS)	General	Human and organizational factors (e.g., awareness, incident response capability) included but not deeply explored; lacks discussion of interactions among determinants
Garba et al. (2020)	Informed by C2M2, ES-C2M2, ONG-C2M2, NICE-C2M2, CCSMM, FFIEC- CMM, and AUMMCS	Mixed sectors	Integrates human and organizational dimensions (e.g., governance, skills, awareness), but lacks empirical testing or cross-sector validation; does not analyze interactions across cybersecurity domains; limited discussion of preparedness outcomes
Latino and Menegoli (2022)	Custom, domain-specific privacy-awareness framework	Food and beverage	Does not apply or assess any standard cybersecurity framework (e.g., NIST, ISO); lacks integration of broader organizational factors; does not evaluate cross-domain interactions or maturity levels; focuses narrowly on immediate outcomes (e.g., system failure probability, attack success rates); does not evaluate intermediate outcomes (e.g., incident response, continuity) or long-term outcomes (e.g., resilience, adaptive capacity)
Georgiadou et al. (2022)	Informed by standards such as PROTECT, NIST SP, and Cybersecurity Culture Framework	Mixed sectors	Emphasizes organizational and human factors; does not assess cross-domain interactions or preparedness outcomes
Aldabjan et al. (2024)	Informed by NSF	Mixed sectors	Integrates technical and policy frameworks but lacks empirical validation; underrepresents human and organizational dynamics (e.g., training, culture, leadership); limited discussion of cross-domain interactions; preparedness outcomes discussed conceptually but not tested (e.g., resilience, adaptability, continuity)
Photipatphiboon et al. (2025)	TOE framework	Mixed sectors	Emphasizes policy and governance but underrepresents technical and operational controls; minimal discussion of cross-domain interactions or preparedness outcomes (e.g., resilience, response capacity); no empirical validation or longitudinal tracking of effectiveness
Chapman and Reithel (2021)	PACRM model, informed by NIST CSF	Education	Focuses on subjective perceptions of readiness rather than objective measures; some evaluation of cross-domain interactions but not comprehensive; no assessment of preparedness outcomes (immediate, intermediate, or long-term); does not track maturity over time
Hasan et al. (2021)	Customized cybersecurity readiness assessment, informed by NIST CSF, ISO/IEC 27001, and ANSI regulations	General	Composite checklist approach lacks empirical validation and sector-specific tailoring; attention to organizational/human dimensions or cross-domain interactions may not be complete; outcomes of preparedness (e.g., response, continuity, recovery) not assessed
Chandra et al. (2022)	Hybrid risk assessment framework based on ISO/IEC 27001	General	Abstract and conceptual with no application to a specific organizational setting; human involvement is present but lacks integration of broader human factors (e.g., culture, leadership, training); focuses on static technical risk identification; does not evaluate preparedness outcomes (e.g., resilience, response, continuity); no cross-domain interaction analysis
Neri et al. (2024)	Informed by NIST CSF, COBIT, ISO/IEC 27001, ENISA	SMEs	Limited operationalization of preparedness outcomes (e.g., recovery, resilience); cross-domain interactions are acknowledged but not quantified; does not use a formal maturity model or track changes over time; human and organizational factors (e.g., awareness, leadership, culture) are discussed conceptually but not comprehensive
Yeoh et al. (2023)	Critical success factor framework	General	Human, organizational, and environmental factors are theoretically modeled but not empirically examined; does not analyze cross-domain interactions;

(*continued on next page*)

Table F.1 (*continued*)

Study	Framework/Approach	Sector/Context	Gaps/Limitations
			outcomes like resilience and response capacity are conceptually modeled but not operationalized or tested; assumes uniform behavior across organizational types
Badi and Nasaj (2023)	Extended McKinsey 7S model (organizational/strategic framework), augmented for cybersecurity	Construction	Integrates human and organizational factors (e.g., skills, structure, leadership) but does not incorporate environmental or technical control domains; assumes interrelations among 7S elements but does not test cross-domain interactions; preparedness outcome (cybersecurity effectiveness) is perception-based
Taherdoost (2022)	Summarizes and compares various frameworks (i.e., ISO/IEC 27000 family, NIST CSF, COBIT)	General	Minimal integration of human and organizational factors beyond compliance and training; no discussion of cross-domain interactions; outcomes of preparedness (e.g., resilience, response capacity) are assumed but not operationalized or assessed

Appendix G: PRISMA Checklist Completion Table

Table G.1
PRISMA Checklist with Corresponding Manuscript Locations

Section and Topic	Item #	Checklist item	Location where item is reported
TITLE			
Title	1	Identify the report as a systematic review.	Page 2 in the abstract; Page 4 in Section 1. Introduction
ABSTRACT			
Abstract	2	See the PRISMA 2020 for Abstracts checklist.	Page 2
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of existing knowledge.	Pages 3–4 in Section 1. Introduction
Objectives	4	Provide an explicit statement of the objective(s) or question(s) the review addresses.	Pages 4–5 in Section 1. Introduction
METHODS			
Eligibility criteria	5	Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses.	Pages 14–17 in Section 3.3 and 3.4
Information sources	6	Specify all databases, registers, websites, organizations, reference lists and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted.	Pages 13–14 in Section 3.2
Search strategy	7	Present the full search strategies for all databases, registers and websites, including any filters and limits used.	Pages 13–14 in Section 3.2; Also see Table 1 and Appendix A
Selection process	8	Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the process.	Pages 14–15 in Section 3.3
Data collection process	9	Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process.	Pages 15–16 in Section 3.4
Data items	10a	List and define all outcomes for which data were sought. Specify whether all results that were compatible with each outcome domain in each study were sought (e.g. for all measures, time points, analyses), and if not, the methods used to decide which results to collect.	Pages 16–17 in Section 3.4
	10b	List and define all other variables for which data were sought (e.g. participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information.	N/A
Study risk of bias assessment	11	Specify the methods used to assess risk of bias in the included studies, including details of the tool(s) used, how many reviewers assessed each study and whether they worked independently, and if applicable, details of automation tools used in the process.	Page 16 in Section 3.4
Effect measures	12	Specify for each outcome the effect measure(s) (e.g. risk ratio, mean difference) used in the synthesis or presentation of results.	N/A
Synthesis methods	13a	Describe the processes used to decide which studies were eligible for each synthesis (e.g. tabulating the study intervention characteristics and comparing against the planned groups for each synthesis (item #5)).	Pages 16–17 in Section 3.4
	13b	Describe any methods required to prepare the data for presentation or synthesis, such as handling of missing summary statistics, or data conversions.	N/A
	13c	Describe any methods used to tabulate or visually display results of individual studies and syntheses.	Page 17–18 in Section 4; Page 37 in Section 4.4
	13d	Describe any methods used to synthesize results and provide a rationale for the choice(s). If meta-analysis was performed, describe the model(s), method(s) to identify the presence and extent of statistical heterogeneity, and software package(s) used.	Pages 16–17 in Section 3.4

(*continued on next page*)

Table G.1 (*continued*)

Section and Topic	Item #	Checklist item	Location where item is reported
	13e	Describe any methods used to explore possible causes of heterogeneity among study results (e.g. subgroup analysis, meta-regression).	N/A
	13f	Describe any sensitivity analyses conducted to assess robustness of the synthesized results.	N/A
Reporting bias assessment	14	Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases).	N/A
Certainty assessment	15	Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome.	N/A
RESULTS			
Study selection	16a	Describe the results of the search and selection process, from the number of records identified in the search to the number of studies included in the review, ideally using a flow diagram.	Pages 13–16 in Sections 3.2-3.3
	16b	Cite studies that might appear to meet the inclusion criteria, but which were excluded, and explain why they were excluded.	Various locations: Articles were excluded if they were duplicate publications, non-English, non-peer-reviewed, did not focus on cybersecurity preparedness, or were tertiary studies.
Study characteristics	17	Cite each included study and present its characteristics.	Pages 17–40 in Section 4. Results from Systematic Literature Review
Risk of bias in studies	18	Present assessments of risk of bias for each included study.	N/A
Results of individual studies	19	For all outcomes, present, for each study: (a) summary statistics for each group (where appropriate) and (b) an effect estimate and its precision (e.g. confidence/credible interval), ideally using structured tables or plots.	N/A
Results of syntheses	20a	For each synthesis, briefly summarise the characteristics and risk of bias among contributing studies.	Pages 17–40 in Section 4. Results from Systematic Literature Review
	20b	Present results of all statistical syntheses conducted. If meta-analysis was done, present for each the summary estimate and its precision (e.g. confidence/credible interval) and measures of statistical heterogeneity. If comparing groups, describe the direction of the effect.	N/A
	20c	Present results of all investigations of possible causes of heterogeneity among study results.	N/A
	20d	Present results of all sensitivity analyses conducted to assess the robustness of the synthesized results.	N/A
Reporting biases	21	Present assessments of risk of bias due to missing results (arising from reporting biases) for each synthesis assessed.	N/A
Certainty of evidence	22	Present assessments of certainty (or confidence) in the body of evidence for each outcome assessed.	N/A
DISCUSSION			
Discussion	23a	Provide a general interpretation of the results in the context of other evidence.	Pages 17–40 in Section 4. Results from Systematic Literature Review
	23b	Discuss any limitations of the evidence included in the review.	Page 45 in Section 6.2
	23c	Discuss any limitations of the review processes used.	Pages 44–45 in Section 6.2
	23d	Discuss implications of the results for practice, policy, and future research.	Pages 40–42 in Section 5; Pages 43–44 in Section 6.1
OTHER INFORMATION			
Registration and protocol	24a	Provide registration information for the review, including register name and registration number, or state that the review was not registered.	Pages 15–16: The review was not pre-registered.
	24b	Indicate where the review protocol can be accessed, or state that a protocol was not prepared.	N/A
	24c	Describe and explain any amendments to information provided at registration or in the protocol.	N/A
Support	25	Describe sources of financial or non-financial support for the review, and the role of the funders or sponsors in the review.	Page 45
Competing interests	26	Declare any competing interests of review authors.	Authors do not have competing interests. This will appear in the final published version.
Availability of data, code and other materials	27	Report which of the following are publicly available and where they can be found: template data collection forms; data extracted from included studies; data used for all analyses; analytic code; any other materials used in the review.	Appendix C

Data availability

We have provided a link to the dataset for this systematic review in the following link:https://docs.google.com/spreadsheets/d/1DMsZVpApSaH-mvCWeWxqhT6E9EpZpXg7lofO_0XHgL8/edit?usp = sharing.

References

Abd El-Latif, A. A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S. E., & Peng, J. (2021). Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in IoT-Based smart cities. *Information Processing & Management, 58*(4), Article 102549.

Abd Rahim, N. H., Hamid, S., & Kiah, M. L. M. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. *Malaysian Journal of Computer Science, 32*(3). Article 3.

Abdelhamid, M., Kisekka, V., & Samonas, S. (2019). Mitigating e-services avoidance: The role of government cybersecurity preparedness. *Information & Computer Security, 27*(1), 26–46.

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons, 62*(4), 539–548.

Acheampong, D., Meso, P., Agyemang, I. O., & Cudjoe, J. (2024). Bridging the digital divide: Securing information and computer systems in an unequal world. In *Implications of information and digital technologies for development*. Springer.

Ahouanmenou, S., Van Looy, A., & Poels, G. (2023). Information security and privacy in hospitals: A literature mapping and review of research gaps. *Informatics for Health and Social Care, 48*(1), 30–46.

Aksnes, D. W., & Sivertsen, G. (2019). A criteria-based assessment of the coverage of scopus and web of science. *Journal of Data and Information Science, 4*(1), 1–21.

Al Amosh, H., & Khatib, S. F. A. (2025). Cybersecurity transparency and firm success: Insights from the Australian landscape. *Australian Economic Papers, 64*(2), 189–204.

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, 13*(10), 5839.

Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. *The Electronic Journal on Information Systems in Developing Countries, 88*(5), Article e12223.

Aldabjan, A., Furnell, S., Carpent, X., & Papadaki, M. (2024). Cybersecurity incident response readiness in organisations. In *Proceedings of the 10th international conference on information systems security and privacy – Volume 1: ICISSP* (pp. 262–269). SciTePress.

Alhalafi, N., & Veeraraghavan, P. (2022). The current state of cyber-readiness of Saudi Arabia. *International Journal of Computer Science and Network Security, 22*(6), 256–274.

Alharbi, N., Papadaki, M., & Dowland, P. (2017). The impact of security and its antecedents in behaviour intention of using e-government services. *Behaviour & Information Technology, 36*(6), 620–636.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences, 10*(10).

Allodi, L., Cremonini, M., Massacci, F., & Shim, W. (2020). Measuring the accuracy of software vulnerability assessments: Experiments with students and professionals. *Empirical Software Engineering, 25*(2), 1063–1094.

AlMindeel, R., & Martins, J. T. (2020). Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Information Technology & People, 34*(2), 770–788.

Alrababah, H., Iqbal, H., & Khan, M. A. (2024). The effect of user behavior in online banking on cybersecurity knowledge. *International Journal of Intelligent Systems, 2024* (1).

Alruwies, M., Mishra, S., Abdul, M., & Alshehri, R. (2022). Identity governance framework for privileged users. *Computer Systems Science and Engineering, 40*.

Althobaiti, M. (2021). Assessing user's susceptibility and awareness of cybersecurity threats. *Intelligent Automation & Soft Computing, 28*(1), 167–177.

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.

Antunes, M., Maximiano, M., & Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. *Applied Sciences, 12*(9), 4102.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437–443.

Ardo, A. A., Bass, J. M., & Gaber, T. (2023). Implications of regulatory policy for building secure agile software in Nigeria: A grounded theory. *The Electronic Journal on Information Systems in Developing Countries, 89*(6), Article e12285.

Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Computers & Security, 105*, Article 102237.

Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., & Medaglia, C. M. (2019). Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Systems Research and Behavioral Science, 36*(4), 404–423.

Armstrong, M. E., Jones, K. S., Namin, A. S., & Newton, D. C. (2020). Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals. *ACM Transactions on Computing Education, 20*(4), 1–25.

Arroyabe, M. F., Arranz, C. F., Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society, 78*, Article 102670.

Auffret, J.-P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., Stein, F., Sokol, L., Allor, P., & Warweg, P. (2017). Cybersecurity leadership: Competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks, 17*(1), Article 1740001.

Badi, S., & Nasaj, M. (2023). Cybersecurity effectiveness in UK construction firms: An extended McKinsey 7S model approach. *Engineering Construction and Architectural Management, 31*(11), 4482–4515.

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

Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0. *Systems, 11*(5), 218.

Batini, C., Cappiello, C., Francalanci, C., & Maurino, A. (2009). Methodologies for data quality assessment and improvement. *ACM Computing Surveys, 41*(3), 16–52.

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability, 13*(24), Article 13761.

Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. *Electronics, 14*(7).

Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A., & Delen, D. (2022). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. *Decision Support Systems, 152*, Article 113651.

Bokhari, S. A. A., & Myeong, S. (2023). The influence of artificial intelligence on E-Governance and cybersecurity in smart cities: A stakeholder's perspective. *IEEE Access, 11*, 69783–69797.

Bongiovanni, I., Renaud, K., Brydon, H., Blignaut, R., & Cavallo, A. (2022). A quantification mechanism for assessing adherence to information security governance guidelines. *Information & Computer Security, 30*(4), 517–548.

Borenius, S., Gopalakrishnan, P., Bertling Tjernberg, L., & Kantola, R. (2022). Expert-guided security risk assessment of evolving power grids. *Energies, 15*(9), 3237.

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change, 67*(3), 265–288.

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*, 1–17.

Caldarulo, M., Welch, E. W., & Feeney, M. K. (2022). Determinants of cyber-incidents among small and medium US cities. *Government Information Quarterly, 39*(3), Article 101703.

Canham, M., Posey, C., Strickland, D., & Constantino, M. (2021). Phishing for long tails: Examining organizational repeat clickers and protective stewards. *Sage Open*, 1–11.

Chandra, N. A., Ramli, K., Ratna, A. A. P., & Gunawan, T. S. (2022). Information security risk assessment using situational awareness frameworks and application tools. *Risks, 10*(8), 165.

Chapman, T. A., & Reithel, B. J. (2021). Perceptions of cybersecurity readiness among workgroup IT managers. *Journal of Computer Information Systems, 61*(5), 438–449.

Chatterjee, D., & Leslie, A. (2024). Ignorance is not bliss: A human-centered whole-of-enterprise approach to cybersecurity preparedness. *Business Horizons*.

Chaudhary, T., Jordan, J., Salomone, M., & Baxter, P. (2018). Patchwork of confusion: The cybersecurity coordination problem. *Journal of Cybersecurity, 4*(1), 1–13.

Chen, J., Zhu, Q., & Başar, T. (2021). Dynamic contract design for systemic cyber risk management of interdependent enterprise networks. *Dynamic Games and Applications, 11*(2), 294–325.

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security, 145*, Article 104026.

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2023). Rushing for security: A document analysis on the sources and effects of time pressure on organizational cybersecurity. *Information & Computer Security, 31*(4), 504–526.

Clark, R. M., Hakim, S., & Panguluri, S. (2018). Protecting water and wastewater utilities from cyber-physical threats. *Water and Environment Journal, 32*(3), 384–391.

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Inc.

De La Cruz, E., Oni, O., Nadella, G. S., Gonaygunta, H., Meduri, S. S., & De La Cruz, A. M. (2024). Cybersecurity data analytics system success: An exploratory study on U.S government agencies. *2024 international seminar on application for technology of information and communication (iSemantic)*.

Delgado, M. F., Esenarro, D., Regalado, F. F. J., & Reategui, M. D. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3 c TIC, 10*(2), 123–141.

Dinkova, M., El-Dardiry, R., & Overvest, B. (2023). Should firms invest more in cybersecurity? *Small Business Economics, 23*(3), 1177–1206.

Dong, B., Chernov, S., & Akpinar, K. O. (2024). Legal aspects of corporate systems for preventing cybercrime among personnel. *Crime, Law and Social Change, 7*(5), 343–359.

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity capacity: Does it matter? *Journal of Information Policy, 9*, 280–306.

Eliza, F., Fadli, R., Ramadhan, M. A., Sutrisno, V. L. P., Hidayah, Y., Hakiki, M., & Dermawan, D. D. (2024). Assessing student readiness for Mobile learning from a cybersecurity perspective. *The Online Journal of Communication and Media Technologies, 14*(4), Article e202452.

Eriksen, M. B., & Frandsen, T. F. (2018). The impact of patient, intervention, comparison, outcome (PICO) as a search strategy tool on literature search quality: A systematic review. *Journal of the Medical Library Association, 106*(4), 420–431.

Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A master attack methodology for an AI-based automated attack planner for smart cities. In *, 6. IEEE Access* (pp. 48360–48373). IEEE Access.

Frandell, A., & Feeney, M. (2022). Cybersecurity threats in local government: A sociotechnical perspective. *The American Review of Public Administration, 52*(8), 558–572.

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2021). Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. *Journal of Accounting and Public Policy, 40*(5), Article 106860.

Fusi, F., Jung, H., & Welch, E. (2023). Technological vulnerability and knowledge of cyber-incidents: Threats to innovativeness in local governments? *Public Management Review*, 1–27.

Garba, A. A., Siraj, M. M., & Othman, S. H. (2020). An explanatory review on cybersecurity capability maturity models. *Advances in Science, Technology and Engineering Systems, 5*(4), 762–769.

Gehanno, J.-F., Rollin, L., & Darmoni, S. (2013). Is the coverage of google scholar enough to be used alone for systematic reviews. *BMC Medical Informatics and Decision Making, 13*(1), 7.

Georgiadou, A., Michalitsi-Psarrou, A., Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Doukas, G., Ntanos, C., Landeiro Ribeiro, L., & Askounis, D. (2021). Hospitals' cybersecurity culture during the COVID-19 crisis. *Healthcare, 9*(10), 1335.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems, 62*(3), 452–462.

Georgieva, I. (2020). The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy, 41*(1), 33–54.

Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022). Towards understanding the skill gap in cybersecurity. *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education, 1*, 477–483.

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*, Article 102726.

Hasani, T., Rezania, D., Levallet, N., O'Reilly, N., & Mohammadi, M. (2023). Privacy enhancing technology adoption and its impact on SMEs' performance. *International Journal of Engineering Business Management, 15*, 1–26.

Hassib, B., & Shires, J. (2021). Manipulating uncertainty: Cybersecurity politics in Egypt. *Journal of Cybersecurity, 7*(1), 1–16.

Hawdon, J., Parti, K., Dearden, T., Vandecar-Burdin, T., Albanese, J., & Gainey, R. (2023). Cybercrime victimization among Virginia businesses: Frequency, vulnerabilities, and consequences of cybervictimization. *Criminal Justice Studies, 36*(3), 269–291.

He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management, 62*, Article 102435.

Hochstetter-Diez, J., Diéguez-Rebolledo, M., Fenner-López, J., & Cachero, C. (2023). AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity. *Applied Sciences, 13*(14), Article 14.

Hong, Y., Kim, M.-J., & Roh, T. (2023). Mitigating the impact of work overload on cybersecurity behavior: The moderating influence of corporate ethics—A mediated moderation analysis. *Sustainability, 15*(19), Article 14327.

Hossain, A., Tin, D., Chum, P., Taing, T., & Chhem, S. (2022). Cybersecurity readiness in developing countries:A survey to demonstrate potential risks of the cambodians. *2022 14th international conference on software, knowledge, information management and applications (SKIMA)*.

Huang, J., & Murthy, U. (2024). The impact of cybersecurity risk management strategy disclosure on investors' judgments and decisions. *International Journal of Accounting Information Systems, 54*, 100696, 17.

Ignatovski, M. (2023). For-profit versus non-profit cybersecurity posture: Breach types and locations in healthcare organisations. *Health Information Management Journal*, 1–8.

Juma'h, A. H., & Alnsour, Y. (2021). How do investors perceive the materiality of data security incidents. *Journal of Global Information Management, 29*(6), 1–32.

Kalogiannidis, S., Paschalidou, M., Kalfas, D., & Chatzitheodoridis, F. (2023). Relationship between cyber security and civil protection in the Greek reality. *Applied Sciences, 13*(4), 2607.

Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal, 32*(4), 888–926.

Kamara, I. (2024). European cybersecurity standardisation: A tale of two solitudes in view of Europe's cyber resilience. *Innovation, 37*(5), 1441–1460.

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital healthcare - Cyberattacks in Asian organizations: An analysis of vulnerabilities, risks, NIST perspectives, and recommendations. *IEEE Access, 10*, 12345–12364.

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers & Security, 127*, Article 103089.

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal, 26*(1), 461–473.

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management, 58*(1), Article 103392.

Khan, N. F., Yaqoob, A., Khan, M. S., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. *Computers & Security, 120*, Article 102826.

Kim, B. J., & Kim, M. J. (2024). The influence of work overload on cybersecurity behavior: A moderated mediation model of psychological contract breach, burnout, and self-efficacy in AI learning such as ChatGPT. *Technology in Society, 77*, 1–13.

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. *Applied Sciences, 13*(6), 3410.

Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy, 14*(3), 417–431.

Kostyuk, N., & Wayne, C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies, 6*(2), 1–25.

Latino, M. E., & Menegoli, M. (2022). Cybersecurity in the food and beverage industry: A reference framework. *Computers in Industry, 141*, Article 103702.

Lee, C. S., & Kim, J. H. (2020). Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts. *Computers & Security, 97*, Article 101995.

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance, 15*(4), 1035–1052.

Li, Y., Goel, S., & Williams, K. J. (2023). Exploring antecedents of professional skepticism on accounting students' performance in cybersecurity. *Journal of Emerging Technologies in Accounting, 20*(1), 147–168.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13–24.

Li, Z., & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly, 35*(1), 151–160.

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports, 5*, Article 100165.

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review, 5*(2), 24–47.

Makridis, C. A., & Smeets, M. (2019). Determinants of cyber readiness. *Journal of Cyber Policy, 4*(1), 72–89.

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security, 95*, 101846.

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security, 27*(2), 233–272.

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting, 6*(3), 63–73.

Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2019). To share or not to share: A behavioral perspective on human participation in security information sharing. *Journal of Cybersecurity, 5*(1), 1–13.

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security, 120*, Article 102820.

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society, 58*, Article 101122.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security, 92*, Article 101731.

Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment. *Information and Computer Security, 32*(1), 38–52.

Neri, M., Niccolini, F., & Pugliese, R. (2022). Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. *Online Journal of Applied Knowledge Management, 10*(2).

Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems, 38*(3), 732–764.

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. *Public Administration Review, 79*(6), 895–904.

Nystad, E., Simensen, J. E., & Raspotnig, C. (2021). Investigating operative cybersecurity awareness in air traffic control. *2021 14th International Conference on Security of Information and Networks (SIN), 1*, 1–8.

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems, 12*(2), 1–29.

Ovchinnikova, O., & Upadhyay, N. K. (2023). The level of cybersecurity of the BRICS member countries in international ratings: Prospects for cooperation. *BRICS Law Journal, 10*(1), 7–34.

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.

Photipatphiboon, P., Chokpiriyawat, T., & Papamo, K. (2025). Cybersecurity readiness in Thailand: The empirical evidence of service sectors. *Edelweiss Applied Science and Technology, 9*(4), 2018–2028.

Piazza, A., Vasudevan, S., & Carr, M. (2023). Cybersecurity in UK universities: Mapping (or managing) threat intelligence sharing within the higher education sector. *Journal of Cybersecurity, 9*(1), 1–15.

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology, 35*(3), 214–231.

Pinto, L. (2022). Assessing the relevance of cybersecurity training and policies to prevent and mitigate the impact of phishing attacks. *Journal of Internet Services and Information Security, 12*(4), 23–38.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work, 24*(2), 371–390.

Porter, T., & Tan, N. (2023). An integrated complex adaptive governmental policy response to cyberthreats. *Journal of Economic Policy Reform, 26*(3), 283–297.

Posey, C., & Folger, R. (2020). An exploratory examination of organizational insiders' descriptive and normative perceptions of cyber-relevant rights and responsibilities. *Computers & Security, 99*, Article 102038.

Rodríguez-Priego, N., van Bavel, R., Vila, J., & Briggs, P. (2020). Framing effects on online security behavior. *Frontiers in Psychology, 11*, Article 527886.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135.

Sapanca, H. F., & Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers' information security awareness levels. *Frontiers in Psychology, 13*, Article 986561.

Schuetz, S. W., Lowry, P. B., Pienta, D. A., & Thatcher, J. B. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems, 37*(3), 723–757.

Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. *IEEE Access, 11*, 87970–87984.

Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks – Undermining public confidence in government. *Journal of Information Technology & Politics, 20*(4), 359–374.

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), Article 101781.

Smith, K. T., Smith, L. M., Burger, M., & Boyle, E. S. (2023). Cyber terrorism cases and stock market valuation effects. *Information & Computer Security, 31*(4), 385–403.

Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems, 43*, Article 100532.

Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management, 34*(4), 1203–1228.

Soylu, D., Medeni, T. D., Andekina, R., Rakhmetova, R., & Ismailova, R. (2021). Identifying the cybercrime awareness of undergraduate and postgraduate students: Example of Kazakhstan. *2021 IEEE international conference on smart information systems and technologies (SIST)*.

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: A cross-country study. *Journal of Global Information Technology Management, 23*(2), 112–137.

Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. (2023). A national survey of hospital cyber attack emergency operation preparedness. *Disaster Medicine and Public Health Preparedness, 17*, 1–4.

Sylvester, F. L. (2022). Mobile device users' susceptibility to phishing attacks. *International Journal of Computer Science and Information Technology, 14*(1), 1–18.

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics, 11*(14), 2181.

Tsado, L., Gibson, C., Alsmadi, I., & Bob, J. (2024). *Cyber ready rural: Understanding law enforcement cyber readiness. 2024 12th international symposium on digital forensics and security (ISDFS)*.

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

Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes, 48*(8), 1565–1585.

Verdugo, J., & Rodríguez, M. (2020). Assessing data cybersecurity using ISO/IEC 25012. *Software Quality Journal, 28*(3), 965–985.

von Skarczinski, B. S., Dreißigacker, A., & Teuteberg, F. (2022). Toward enhancing the information base on costs of cyber incidents: Implications from literature and a large-scale survey conducted in Germany. *Organizational Cybersecurity Journal: Practice, Process and People, 2*(2), 79–112.

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.

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, 102520.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93–112.

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers & Security, 133*, Article 103412.

Yoo, C., Goo, J., & Rao, R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly, 44*(2), 907–931.

Younies, H., & Al-Tawil, T. N. (2020). Effect of cybercrime laws on protecting citizens and businesses in the united arab emirates (UAE). *Journal of Financial Crime, 27*(4), 1089–1105.

Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society, 19*(4), 446–462.

Zainudin, Z. S., & Nuha Abdul Molok, N. (2018). Advanced persistent threats awareness and readiness: A case study in Malaysian financial institutions. *2018 cyber resilience conference*. CRC).

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169–187.