Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Breach to Resilience: A Conceptual Review of Multi-case Global Cyberattacks

Emmanuel Olufemi Igbekele

emmanuel.igbekele@up.ac.za

University of Pretoria

Grace Funmilayo Smith

Landmark University

Olumide Victor Adams

Landmark University

Research Article

Keywords: Cyber-resilience, Zero Trust Architectures, Risk Assessment, Incident Response

Posted Date: June 29th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9009078/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Modern Information Technology ecosystems have been created to solve several organizational technological problems. However, in doing so, they have successfully broadened the threat landscape, leaving them vulnerable to more strategic and sophisticated cyberattacks. This increase in susceptibility to attacks has spotlighted the insufficiency of the traditional security models while underscoring the need to migrate to more proactive and adaptive approaches to security. As a result, cyber resilience is gaining more attention as a strategy that fully supports an organization's ability to detect, withstand, respond to, and recover from cyber incidents. This paper presents a conceptual narrative review of literature published between 2020 and 2025, centered on the need for and improvement of cyber resilience. This review combines existing research on cyber resilience and lessons from documented cyber incidents. It reveals the gaps in existing literature and contributes to a clearer understanding of cyber resilience through the formulation of its own four-tier framework.

1 Introduction

Information Technology systems have greatly evolved into a more interconnected digital infrastructure and one of the biggest signs of this growth is the simultaneous enlargement of the cyber threat landscape. The artificial intelligence, cloud based and internet-connected services pose the risk of becoming an additional threat vector going on to disrupt critical services and affect several national economies [1,2]. The traditional security models are heavily focused on prevention, emphasizing perimeter defenses. However, they are very unfamiliar with this more recent wave of cyber threats, cyber risks and cyber-attacks so it is simply impossible for them to defend against it [3]. The high-profile breaches that have occurred in recent times have shown that even well-protected organizations can fall victim. The rate of successful breaches goes to show that prevention is now an unrealistic goal and organizations should focus on smooth operations and minimal impact when these breaches do occur (cyber resilience).

Most frameworks still address certain sectors specifically and over-technicality ignoring the socio-technical aspects of cyber resilience such as human behavior, the organizations' readiness and collaboration across all sectors [4]. Indeed, there is a need for organizations to review on their cyber resilience strategies focusing on the ability to detect, withstand, respond to, and recover from cyber incidents. This conceptual review adopts a broader view that goes beyond specificity in sectors and attacks and shows persistence over time so that there can be a more general approach for building stronger cybersecurity foundations.

2 Materials and Methods

2.1 Cyber-Resilience

Cybersecurity is a combination of technologies, processes, and practices that aim to protect networks, systems, and data from cyberattacks and unauthorized access [5]. Cyber resilience refers to an organization's ability to prepare for, respond to and recover from cyberattacks while ensuring business continuity [2]. Others describe it as the capacity of socio-technical systems to adapt to, recover from and evolve when cyber incidents occur [6]. Cyber resilience emphasizes on the fact that attacks will happen and focuses on reducing the impact that these attacks have on an organization and recovery speed [7].

This framework will particularly be evaluating resilience across four stages: Preparedness, Detection and Response, Resistance as well as Recovery and Adaptation. Preparedness being that the occurrence of cyberattacks is expected and plans are made to that effect. Detection and Response involves the identification of early signs of cyberattacks so that timely decisions can be made. Resistance evaluates how an organization can reduce the impact of cyberattacks while simultaneously preventing escalation. Lastly, recovery and adaptation relate to the ability of the organization to adapt to how operations need to run during the period of the attack, recover from it and learn to improve future resilience.

2.2 Research Questions

The review curated two clear, focused, and arguable questions that helped drive the study, defining its scope and directing data collection, thereby transforming the topic into a specific inquiry, helping us to fill gaps in knowledge.

RQ1: What lessons can be learned from documented cyberattacks to improve or-ganizational cyber resilience?

RQ2: What gaps exists in current cyber resilience research that justifies the need for a unified conceptual framework.

2.3 Reasons for considering studies in this review

This research emphasizes on how organizations respond to and manage cyber incidents as well as the resilience frameworks they have in place. The research questions and keywords align directly with the problem definition, focusing on preparedness, detection and response, resistance, and recovery and adaptation. The purpose of this review is to evaluate organizational cyber resilience through the examination of multiple global cyberattacks and synthesize existing literature on the topic to formulate a unified resilience framework.

These studies were selected because of their relevance to organizational cyber re-silience and how cyber incidents are managed. Journal articles, international standards, industry publications and government reports between 2020 and 2026 were prioritized as depicted in Fig. 1. A few inclusion and exclusion strategies were deployed as depicted in Table 1.

Table 1
Consideration for inclusion and exclusion in this review.

SN	Inclusion Criteria	Exclusion Criteria
1.	Studies published between 2020 and 2026	Studies published before 2020
2.	Articles written in English	Articles written in other languages
3.	Studies focusing on cyber resilience, organizational cybersecurity, incident response, recovery strategies, or major cyber incidents	Studies not related to cybersecurity, cyber resilience, or organizational security
4.	Full text available through reputable databases, official websites, or institutional access for verification.	Sources lacking sufficient methodological detail, case study specifics, or technical depth.

2.4 Strategies for searching for relevant publications

The literatures used for this review were curated through thorough search of various academic databases and reputable sources. These databases include IEEE Xplore, Scopus, Web of Science, SpringerLink, and Google Scholar and other sources such as NIST, ENISA, CISA, IBM, Verizon, Trend Micro, and Microsoft Security Response Center were also used. The following categories of interest were used for the search terms: Cybersecurity, Cyber resilience and incident response, human and organizational factors in cybersecurity, threat detection and cyber threats. Boolean operators “AND” and “OR” were also used to combine terms effectively.

3 Results

The search process was meticulous and afterwards, 17 articles and papers published between 2020 and 2025 were included in this review. The studies were analyzed, common patterns were identified and results of the findings were compared. These findings were grouped into four major sections aligned with cyber resilience as mentioned above: Preparedness, Detection and Response, Resistance, and Recovery and Adaptation. They fit perfectly with the proposed cyber resilience framework. The variation is depicted in Table 2.

Table 2
Distribution of Reviewed Studies Across Cyber Resilience Stages

Authors	Preparedness	Detection & Response	Resistance	Recovery & Adaptation
[2]	Y	Y	Y	N
[3]	Y	Y	N	N
[5]	N	N	N	Y
[6]	Y	Y	Y	Y
[8]	Y	Y	Y	Y
[9]	Y	Y	Y	N
[10]	Y	Y	Y	N
[11]	Y	Y	Y	N
[12]	Y	N	Y	Y
[13]	Y	Y	Y	N
[14]	Y	Y	Y	N
[15]	Y	Y	Y	N
[16]	Y	Y	Y	N
[17]	N	Y	Y	N
[18]	Y	Y	Y	N
[19]	Y	Y	Y	N
[20]	Y	Y	Y	N
[21]	Y	Y	N	Y

[Y]: Yes [N]: No

As shown in the table above, these studies focus majorly on preparedness, detection and response and also resistance. However, very few have incorporated the need for recovery and adaptive resilience. Furthermore, none of them have been able to capture and adequately address all four stages. This imbalance emphasizes the need for a unified integrated framework that surpasses prevention and basic incident response. Hence, Table 3 shows a summary of the identified gaps under the selected cyber resilience sections.

Table 3
Distribution of Reviewed Studies Across Cyber Resilience Stages.

Resilience Stage	Identified Gaps	Corresponding Study
Preparedness	Limited predictive capabilities and overreliance on technical controls	[2], [3], [12]
Detection & Response	Delayed detection as opposed to anticipation of zero-day attacks, limited human-AI coordination and insufficiency of signature-based methods.	[6], [15], [17]
Resistance	Difficulty implementing Zero Trust in legacy systems, weak segmentation in industrial networks, supply-chain interdependence risks	[9], [14], [16]
Recovery & Adaptation	Lack of operational recovery models, limited post-incident learning frameworks, insufficient integration of human-AI collaboration	[6], [8], [21]

These results depicted in Tables 3 and Fig. 2 shows that the concept of adaptive recovery is still struggled with. Likewise, getting human and AI systems to work together more efficiently and coming up with security models that apply to all organizations re-gardless of size and sector.

3.1 Research Challenges

Several challenges were encountered during the course of this review. Firstly, different papers defined cyber resilience differently; some focused on technicalities and others focused on people. This inconsistency made comparison between the studies difficult. Also, a lot of the research was centered around the “before” and “during” of the cyber incidents without enough information on what happened after. Furthermore, several companies are not too keen on disclosing security failures so a lot of researchers end up basing their work on best guesses and simulations. Finally, humans and technology are treated as separate entities in existing literature and as such, there is limited research on their interaction during the course of these cyber incidents. In conclusion, there is limited research on the socio-technical nature of organizational cyber resilience. Figure 3 depicts the strategy for identifying the selected reviewed articles

4 Discussion

Findings from this review presents a structured, critical synthesis of existing cyber-resilience strategies, highlighting key outcomes, and the certainty of evidence. These findings summarize the magnitude of cyberattacks, provides answers to our research questions, and proposes areas that still needs future research efforts.

4.1 Research Questions Answered

Findings from this review are as follow:

RQ1: *What lessons can be learned from documented cyberattacks to improve organizational cyber resilience*?

The major lessons learnt include the need for stronger security strategies for supply chains. Faster detection mechanisms are also very important alongside an integrated recovery plan. These plans should be formulated such that they can run without affecting each other or disrupting operations and they should also involve human factors like decision making in all stages.

RQ2: *What gaps exist in current cyber resilience research that justify the need for a unified conceptual framework*?

Current research lacks a unified multi-stage resilience framework that combines technical, organizational and human dimensions across all the resilience stages that this research elicits: preparedness, detection and response, resistance and recovery and adaptation. Instead of having one standard system, information is scattered and there is a severe lack of cross sector collaboration in the world at large. This justifies the need for a unified integrated cyber resilience model.

4.2 Summary of Findings

Despite all the extensive work reviewed on cyber resilience, there remains several critical gaps that this review highlighted. The conversations around these studies focused on keeping an attacker out rather than how to keep uninterrupted service regardless of an attack. It is clearly shown that there is a very good understanding of the different technical defenses, but the idea of adaptive cyber resilience still exists more in theory than practice. There is also the issue of cyber inequality. Studies have remained unable to focus evenly on security across sectors. As much as research adapts some lessons from major global cyberattacks, there is still no record of it being applied to the resources and constraints on small and medium enterprises (SMEs).

It is these SMEs that develop into the global enterprises that we see today and if these lessons cannot apply to them now, it makes it harder to apply to them when they scale up. Furthermore, while many studies talk about how much AI is being used, not many of them really address how well humans and AI systems can work together. It would be an oversight to keep treating technicalities and human factors as separate issues. Also, many studies address these cyber incidents in isolation or small clusters.

5 Conclusion

This review set out to examine how organizational cyber resilience is defined, implemented, and studied in recent literature published between 2020 and 2026. It combines its findings to provide a centralized understanding of how organizations prepare for, detect, withstand, respond to, and recover from cyber threats. The findings show the importance of operational continuity in the cyber resilience life cycle while highlighting the need to integrate human decision-making with artificial intelligence for cyber defense.

The review reveals persistent weaknesses in recovery and adaptation, which remain under-represented in both academic research and practical frameworks.

Overall, this review identifies a clear gap in current research: the absence of a unified conceptual framework that integrates preparedness, detection and response, resistance, and recovery and adaptation into a single operational model.

Declarations

Funding:

The APC was funded by Landmark University.

Author Contribution

Conceptualization, E.I. and S.G.; Methodology, E.I. and S.G.; Validation, E.I. and S.G.; Resources, E.I.; Data curation, S.G.; Writing—original draft preparation, S.G.; Writing—review and editing, E.I and O.A.; Supervision, E.I.; Project administration, E.I.; Funding acquisition, E.I. and O.A.

Acknowledgments:

During the preparation of this review, the author(s) used Consensus AI for the purposes of Identification of key domains of cyber resilience. The authors have reviewed and edited the output and take full responsibility for the content of this publication."

Data Availability

Not Applicable

References

1. IBM Security, Cost of a Data Breach Report 2024, 2023. https://www.ibm.com/reports/data-breach
2. I. Alhassan, M. G. Samaila, and S. Islam, "A systematic review of organizational cybersecurity risk management: Challenges and strategies," Computers & Security, vol. 114, p. 102579, 2022. https://doi.org/10.1016/j.cose.2021.102579
3. I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: Current and prospects," Annals of Data Science, vol. 10, pp. 1473–1498, 2022. (PDF) Cybersecurity data science: an overview from machine learning perspective

4. Araujo, M. S. de, B. A. S. Machado, and F. U. Passos, “Resilience in the context of cyber security: A review of the fundamental concepts and relevance,” Applied Sciences, vol. 14, no. 5, p. 2116, 2024. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance | MDPI
5. I. Tiutiunyk, A. Kuzior, A. Zielińska, and R. Kelemen, “Cybersecurity and cybercrime: Current trends and threats,” Journal of International Studies, vol. 17, no. 2, pp. 220–239, 2024. Cybersecurity and cybercrime: Current trends and threats
6. J. Fernández-Miguel et al., “From resilience to cognitive adaptivity: Redefining human–AI cybersecurity,” Information, vol. 16, no. 10, p. 881, 2025. From Resilience to Cognitive Adaptivity: Redefining Human–AI Cybersecurity for Hard-to-Abate Industries in the Industry 5.0–6.0 Transition
7. World Economic Forum, Global Cybersecurity Outlook 2023, 2023. https://www.weforum.org
8. S. Srinivasan and J. Ni, “Cyber resilience of critical energy infrastructure: The Colonial Pipeline case,” UNECE Group of Experts on Energy Efficiency, 2023. Ransomware Attack at Colonial Pipeline Company - Case - Faculty & Research - Harvard Business School
9. G. Stergiopoulos, D. Gritzalis, and E. Limnaios, “Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns,” IEEE Access, vol. 8, pp. 128440–128475, 2020.’ Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns | IEEE Journals & Magazine | IEEE Xplore
10. V. R. K. Adapa, “Zero trust architecture implementation in enterprise networks: Evaluating effectiveness against cyber threats,” International Journal of Computer Applications, vol. 187, no. 45, 2024. (PDF) ZERO TRUST ARCHITECTURE IMPLEMENTATION IN CRITICAL INFRASTRUCTURE: A FRAMEWORK FOR RESILIENT ENTERPRISE SECURITY
11. M. Al-Hawawreh, M. Alazab, M. A. Ferrag, and M. S. Hossain, “Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis,” Journal of Network and Computer Applications, vol. 223, p. 103809, 2023. Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms | Request PDF
12. M. A. Çifci and E. Erdem, “Analysis of national cybersecurity strategies of G20: A data-driven policy perspective,” Data & Policy, vol. 7, p. e12, 2025. Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons | Data & Policy | Cambridge Core
13. N. T. Y. Elete, “Impact of ransomware on industrial control systems in the oil and gas sector: Security challenges and strategic mitigations,” Computer Science & IT Research Journal, vol. 5, no. 12, pp. 2664–2681, 2024. Impact of ransomware on industrial... preview & related info | Mendeley
14. J. Fernandez and A. Brazhuk, “A critical analysis of Zero Trust Architecture (ZTA),” Computer Standards & Interfaces, vol. 89, p. 103832, 2024. (PDF) A Critical Analysis of Zero Trust Architecture (Zta)
15. M. Dosumu, “MOVEit data breach: Analysis, proposed solution, and prevention strategies,” ResearchGate, 2024. (PDF) MOVEit Data Breach: A Case Study in Zero-Day Exploits and

Organizational Cybersecurity Preparedness

16. Y. He et al., “A survey on Zero Trust Architecture: Challenges and future trends,” Wireless Communications and Mobile Computing, vol. 2022, Article ID 6476274, 2022. (PDF) A Survey on Zero Trust Architecture: Challenges and Future Trends
17. R. Holdbrook, O. Odeyomi, S. Yi, and K. Roy, “Network-based intrusion detection for industrial and robotics systems: A comprehensive survey,” Electronics, vol. 13, no. 22, p. 4440, 2024. Network-Based Intrusion Detection for Industrial and Robotics Systems: A Comprehensive Survey
18. J. Kang et al., “Theory and application of zero trust security: A brief survey,” Entropy, vol. 25, no. 12, p. 1595, 2023. Theory and Application of Zero Trust Security: A Brief Survey
19. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800 – 207, National Institute of Standards and Technology, 2020. SP 800 – 207, Zero Trust Architecture | CSRC
20. A. Zanasi et al., “Flexible zero trust architecture for industrial IoT cybersecurity,” Ad Hoc Networks, vol. 156, p. 103414, 2024. (PDF) Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures
21. S. Khadka and A. Ullah, “Human factors in cybersecurity: An interdisciplinary review,” International Journal of Information Security, 2025. Human factors in cybersecurity: an interdisciplinary review and framework proposal | International Journal of Information Security.

Figures

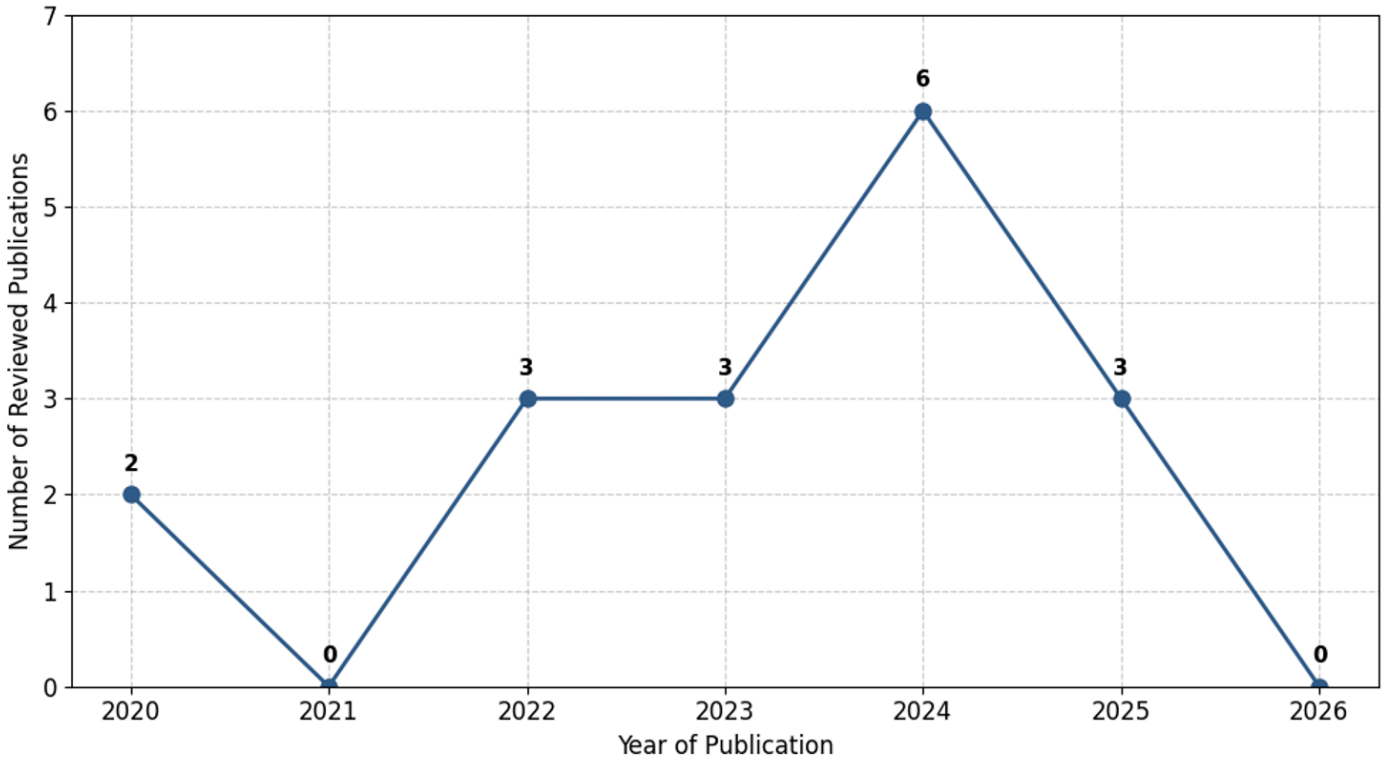

Figure 1

Publication Trend on Organizational Cyber Resilience

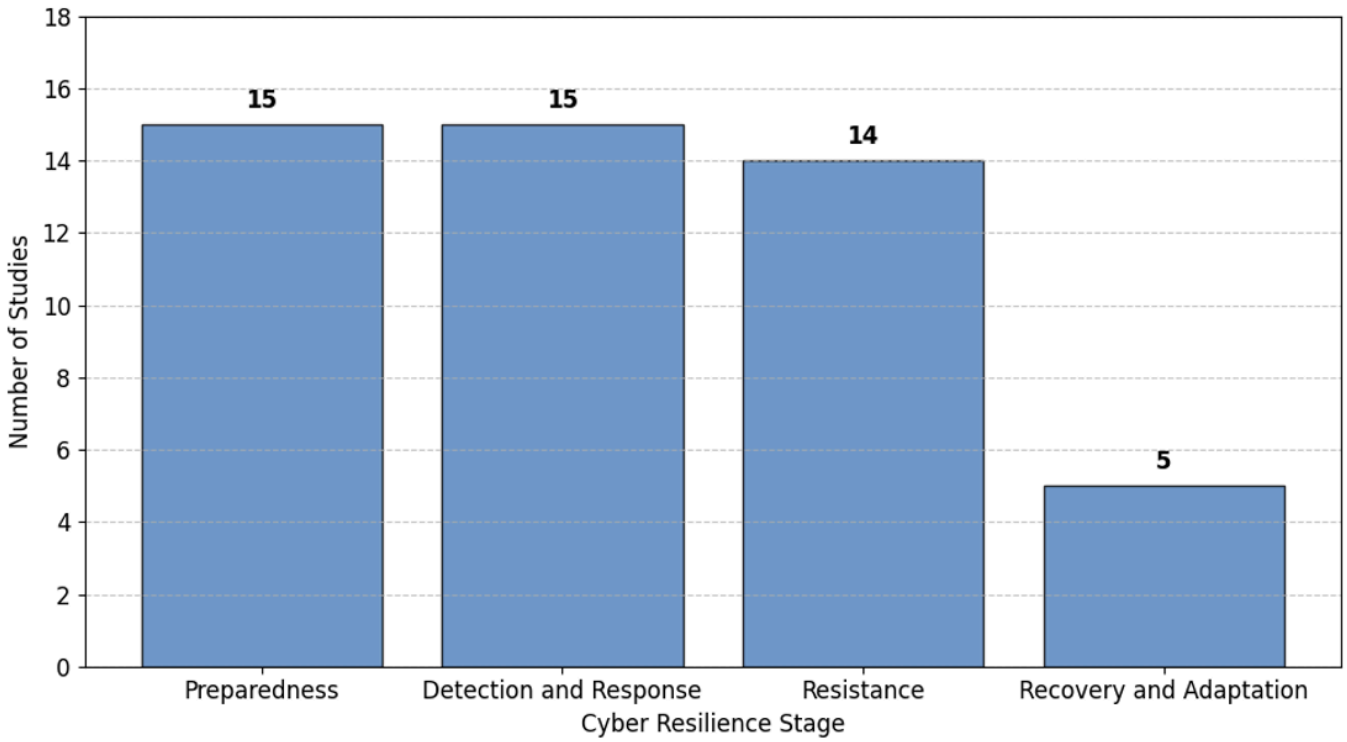

Figure 2

Distribution of Reviewed Studies Across Cyber Resilience Stages.

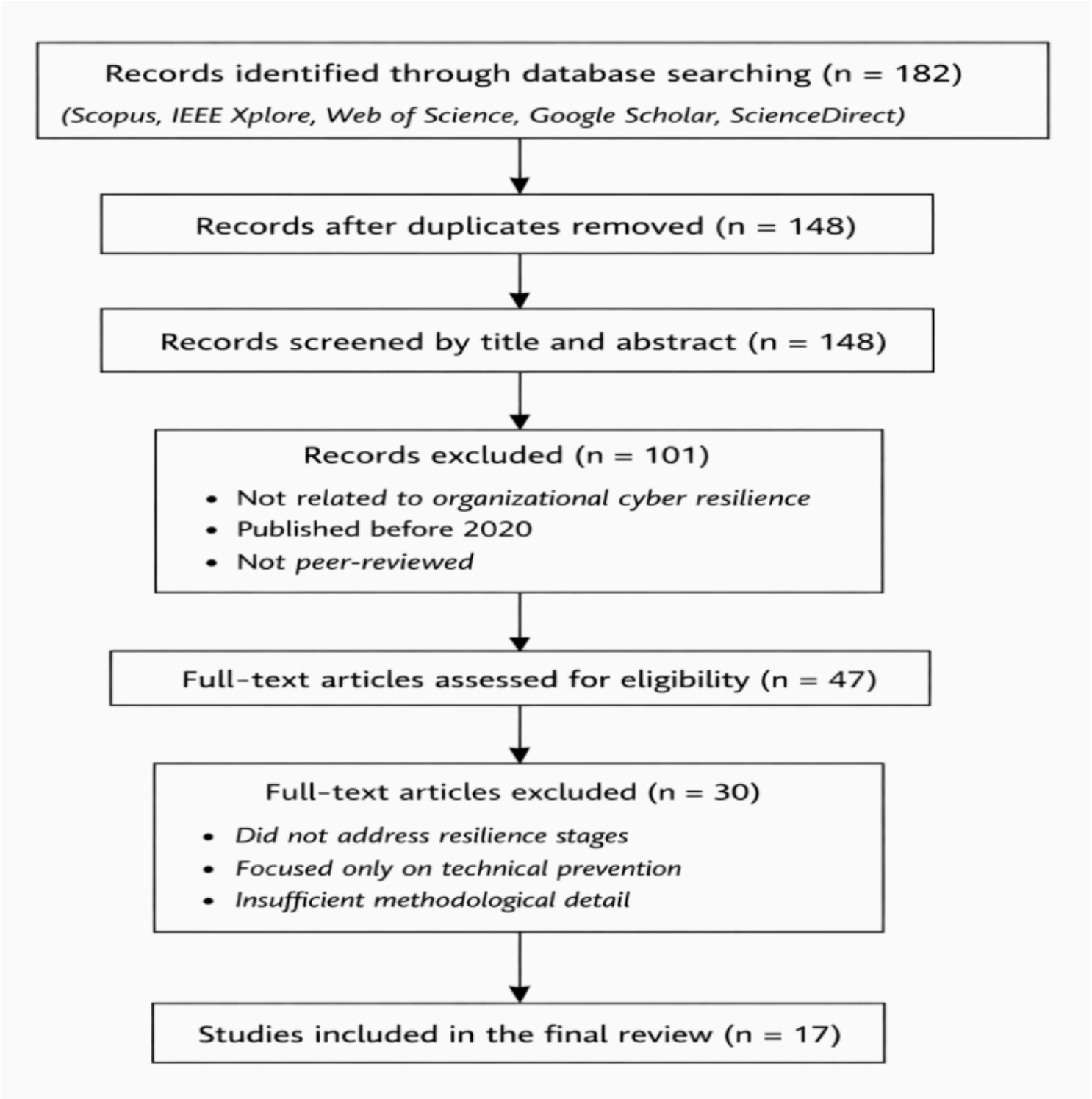

Figure 3

Study Selection Process for the Conceptual Review