P-ISSN: 2709-6254	Journal of Development and Social Sciences	October-Dec 2024, Vol. 5, No. 4
O-ISSN:2709-6262	https://doi.org/10.47205/jdss.2024(5-IV)64	[728-742]

Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

Building Cyber Resilience: Strategies for Anticipating, Withstanding, and Recovering from Digital Threats

Sohail Naseer
MS Finance, Air University School of Management, Air University, Islamabad, Pakistan
***Corresponding Author:** sohailnaseercp@yahoo.com

ABSTRACT

Organizations increasingly frame cybersecurity not only in terms of prevention but of resilience — the capacity to anticipate, withstand, and recover from digital threats. This systematic literature review synthesizes 106 studies identified from IEEE Xplore, ACM Digital Library, and Google Scholar (980 unique records screened from 1,023 raw exported/downloaded records; Scopus and Web of Science were not accessible and are excluded from scope) to characterize the strategies, research methods, and evidence gaps in this literature, organized around a three-phase classification (Anticipate, Withstand, Recover) with Adaptation examined as a cross-cutting theme. Anticipate-phase research is the most mature, dominated by cyber threat intelligence production/sharing and situational-awareness architectures for critical infrastructure. Withstand-phase research is comparatively fragmented across Zero Trust architectures, cyber-physical-system attack detection, and resilience-by-design engineering. Recover-phase research, initially the thinnest phase in an interim analysis, proved substantially better represented once the full evidence base was assembled, combining mature technical work on ransomware detection/recovery and disaster recovery with organizational research on incident-response-team establishment. Framework/model proposals and simulation/technical evaluations together account for 53% of included studies, while empirical organizational research accounts for only 14% — a field stronger at proposing and technically validating mechanisms than at empirically observing organizational practice. Post-incident crisis communication, independent replication of newly proposed technical mechanisms, and empirical study of organizational adaptation over time are the most concretely evidenced gaps for future research. Methodological limitations — incomplete database coverage, an evidenced false-positive rate in automated screening, and single-reviewer screening/extraction — are reported explicitly rather than smoothed over.

KEYWORDS Cyber Resilience, Cyber Resiliency Framework, Cybersecurity, Systematic Literature Review, PRISMA, Cyber Threat Intelligence, Incident Response, Organizational Resilience

Introduction

Organizations' exposure to cyber threats continues to grow in scale and cost even as detection and response capabilities improve. IBM's *Cost of a Data Breach Report* — Ponemon Institute research across 600 breached organizations — found the global average breach cost at USD 4.44 million, a 9% decline attributed largely to faster, AI-aided detection and containment (mean time to identify and contain fell to 241 days, a nine-year low). The same report surfaces a new risk dimension: 13% of organizations experienced attacks impacting AI models or applications, high-"shadow AI" organizations incurred USD 670,000 in additional breach costs on average, and 97% of organizations with an AI-related incident lacked proper AI access controls.

The World Economic Forum's *Global Cybersecurity Outlook* (with Accenture) reinforces that this is not simply a story of improving defenses. Ninety-four percent of respondents identified AI as the most significant driver of cybersecurity change, and the share of organizations formally assessing AI-specific risk nearly doubled (37% to 64%). Confidence in national cyber preparedness moved in the wrong direction — 31% reported low confidence, up from 26% the prior year — with sharp regional disparities (84% in the

Middle East/North Africa versus 13% in Latin America and the Caribbean) and public-sector organizations reporting insufficient resilience capabilities at a higher rate (23%) than other sectors. Together, these reports motivate this review's premise: the challenge is no longer simply preventing breach but continuing to operate and recovering quickly when — not if — one occurs, and organizational confidence in that capacity is, by the latest data, uneven and in places declining.

From cybersecurity to cyber resilience

The U.S. National Institute of Standards and Technology (NIST) defines **cyber resiliency** as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources," intended to let mission or business objectives be achieved even in a contested cyber environment — that is, resiliency assumes some attacks will succeed rather than assuming all can be prevented (NIST SP 800-160, Vol. 2, Rev. 1; Ross et al., 2021). This four-part anticipate/withstand/recover/adapt structure originates in the MITRE Cyber Resiliency Engineering Framework, traced in detail by this review's own included literature (Bodeau & Graubart, 2011; Bodeau et al., 2014a). It is the direct basis for this review's own classification scheme: three of the four dimensions — **Anticipate, Withstand, and Recover** — are named in the title and organize the synthesis, while the fourth, **Adaptation**, is examined separately as a cross-cutting theme in Section 5.2, because the included literature engages with it far less directly and consistently than the other three.

Cyber resilience is thus conceptually distinct from, though complementary to, conventional cybersecurity's historical emphasis on prevention (Bodeau, 2018). Resilience assumes breach is likely for a sufficiently motivated adversary and asks how quickly and completely an organization detects, contains, operates through, and recovers from it — and how it changes posture afterward. This is the lens applied to 106 studies retrieved from IEEE Xplore, ACM Digital Library, and Google Scholar.

The gap this review addresses

The literature on cyber resilience strategies is fragmented across disciplinary silos — threat-intelligence researchers, incident-response-management researchers, ransomware-recovery researchers, and organizational-resilience-framework researchers largely publish within their own venues, with limited synthesis connecting anticipatory strategies to withstand-phase mechanisms to recovery-phase practice within one consistent scheme. This review's own evidence base illustrates the point: only 14% of the 106 included studies are genuinely empirical organizational research (Section 4.1), with the rest split between framework/model proposals (31%) and technical simulations (22%) that rarely cite across the anticipate/withstand/recover boundary. This review addresses that fragmentation by applying one consistent three-phase scheme across a systematically identified, screened, and full-text-assessed evidence base.

Structure of this review

Section 2 (Literature Review) synthesizes the 106 included studies by phase — Anticipate, Withstand, Recover, and cross-cutting/framework literature — addressing RQ1. Section 3 (Methodology) describes the search, screening, and eligibility process and its retrieval limitations. Section 4 (Results) addresses RQ2's method-distribution question and RQ3's gap analysis. Section 5 (Conclusion) revisits all three RQs, introduces Adaptation as a cross-cutting theme, states this review's limitations, and synthesizes overall findings. Section 6 (Recommendation) closes with the most concretely evidenced directions for future research.

Literature Review

Because a study can span more than one phase, the 106 included studies are described in two layers: how many touch each phase at all (inclusive; the four phase counts sum to more than 106), and how many treat a single phase as sole focus (exclusive; sums to 106 together with multi-phase studies).

Table 1
Phase distribution across the 106 included studies (studies may touch more than one phase).

Phase	Studies touching this phase (inclusive)	Studies with this as sole focus
Anticipate	55	29
Withstand	29	9
Recover	28	5
Cross-cutting / framework	41	30

The remaining 33 studies span two or more phases jointly. Anticipate is the most heavily represented phase (52%), and cross-cutting/framework literature is also large (39%). Recover (26%) includes a genuine cluster of ransomware detection-and-recovery systems, disaster-recovery architectures, and organizational CSIRT-establishment literature (Section 2.4). This distribution (Table 1) describes the studies actually synthesized, not a claim about the complete population of 980 screened records — 362 screened-relevant records were never retrieved (Section 3.2), and the observed false-positive rate suggests a meaningful fraction of those would not have been eligible even if retrieved.

The 106 included studies are drawn fairly evenly across the three searchable databases: ACM Digital Library direct search contributed the largest single share (32), followed by IEEE Xplore (29), Google Scholar (23), and ACM Digital Library via Crossref (22).

Anticipate: strategies and mechanisms

The Anticipate literature spans several sub-themes. **Cyber threat intelligence (CTI)** work covers automated extraction of structured intelligence and MITRE ATT&CK TTPs from text (Chen et al., 2023), threat attribution via graph representation learning and DNS pattern analysis (Duan et al., 2023), and organizational CTI-sharing challenges, quality assurance, and tradecraft (Saeed et al., 2023).

Cyber situational awareness and incident correlation is a second major cluster: VSM-based correlation linking incident reports, vulnerability alerts, and threat advisories for critical-infrastructure protection (Settanni et al., 2016); combined situational-awareness models for cyber-physical monitoring operators (Timonen, 2015); smart-grid attack-scenario analysis with security-by-design countermeasures (Shovgenya et al., 2015); an empirical finding that CTI analysts' limited access to tacit "threat and defence knowledge" reduces their ability to anticipate threats (Ahrend et al., 2016); and event-correlation frameworks addressing gaps in standardized CTI sharing (Kim et al., 2016; Cho et al., 2016; Padayachee & Worku, 2017).

A third, smaller cluster addresses **vulnerability/risk assessment and standards alignment** — attack-surface reduction, OSINT integration, and framework alignment against NIST CSF, ISO 27001, and IEC 61511/62443 (Porter et al., 2022; Rommel et al., 2023; Gabriel et al., 2017; Mavroeidis & Bromander, 2017; Silva & Barros, 2017; Nykänen & Kärkkäinen, 2016; Khou et al., 2017a/b), including Nguyen, Shen & Thai (2013), whose proactive critical-node-identification algorithm for cascading-blackout prevention required a manual eligibility override after an initial classifier misread of its adversarial-attack framing.

Two uncertainty flags apply: the CTI literature's volume may partly reflect which venues were searchable rather than representativeness, and Burton (2016), on cyber-attacks and maritime situational awareness, sits closer to international-relations analysis than organizational cyber-resilience practice — retained at eligibility but weighted accordingly.

Withstand: strategies and mechanisms

The Withstand literature (29 studies touching; 9 sole focus) clusters around three sub-themes. **Zero Trust architecture**: challenge-response software-integrity authentication and integration with the MITRE ATT&CK matrix for public-sector detection/response. **Cyber-physical systems (CPS) resilience**: smart-grid Automatic Generation Control detection (Nafees et al., 2021), attack mitigation in delay-tolerant networks, a systematization of CPS detection-reaction techniques, a controller-diversification mechanism spanning Withstand and Recover, and a multi-layered deep-learning detector for SCADA gas-pipeline attacks achieving 96.5% detection accuracy with a 0% false-alarm rate (Eke et al., 2020). **Security-operations infrastructure**: real-time graph-based threat-intelligence generation and a decentralized multi-agent SIEM-replacement architecture. **Engineering-level mechanisms**: language/toolchain design choices to reduce exploitable defects (Wheeler, 2019); deterministic-replica state-comparison for detecting hardware or cyber-attack divergence (Troiani, 2020); Time Petri Net extensions modeling attack-timing impact on mission-critical assets (Cam & Mouallem, 2013); and a Cyber Resilience Engineering Framework building resilience "by construction" via Algebraic Petri nets, demonstrated on a firewall case study (Khan et al., 2015).

Recover: strategies and mechanisms

The 106-study set includes 28 studies touching Recover (5 sole focus), across three sub-clusters. **Ransomware detection and recovery**: a hypervisor/SSD tag-based approach evaluated on 3,123 real ransomware samples with full file restoration (Ma et al., 2023); a comparison of four backup technologies against ransomware/disaster-recovery criteria (Singhal, 2022); a response framework built from reverse-engineering 25 ransomware variants, arguing existing defenses over-focus on detection while recovery guidance is neglected (Bajpai & Enbody, 2023); an SSD DRAM-cache-based detector/recovery mechanism with faster detection and a smaller recovery queue; and an early-stage parallel-blockchain architecture for SCADA historian data that candidly reports remaining vulnerability to ransomware-induced corruption.

Disaster recovery and business continuity: Disaster-Recovery-as-a-Service for SMEs, weighed against named risks of cloud-based DR tied to privileged malicious actors (Ben Rebah & Ben Sta, 2016); an enterprise data-asset architecture combining DR backup with AI-based threat detection; and an evaluation of the GRR incident-response/forensics framework in simulated healthcare, effective for live forensics but flagging a genuine HIPAA/PHI exposure risk in its default settings (Acharya et al., 2015).

Organizational incident-response capability: a two-part CSIRT-capability management model (Mooi & Botha, 2016a) applied to establish South Africa's national research-network CSIRT across roughly 204 institutions (Mooi & Botha, 2016b); a systematic review of CSIRT services from 37 primary studies (Mejia et al., 2015); a fuzzy-logic incident-detection method with CERT/CSIRT effectiveness baselines (Gizun et al., 2015); an analysis of Pakistan's national incident-response capability gaps with a multi-tier roadmap (Tariq et al., 2013); an empirical finding that national CSIRTs lack a generally accepted standard for evaluating their own tools (Kassim et al., 2023); expert-interview-derived requirements for machine-readable incident-response playbooks; and a Systemic Design study of sociotechnical factors in CSIRT effectiveness and analyst burnout, reporting preliminary findings.

No study treats **post-incident crisis communication** as its primary contribution — a narrow but real gap despite otherwise substantial Recover coverage.

Cross-cutting and framework literature

The cross-cutting/framework cluster (41 touching; 30 sole focus) spans several strands. The **MITRE Cyber Resiliency Engineering Framework (CREF) lineage** is the most direct precedent for this review's own model: Bodeau et al. (2011, 2014a; Bodeau, 2018) establish four goals — Anticipate, Withstand, Recover, and Evolve — the last treated here as part of the cross-cutting Adaptation theme (Section 5.2); Bodeau et al. (2014b) extend the structure to systems-of-systems in the space domain; Ross et al. (2019) extends it into systems-security-engineering guidance for building resiliency against Advanced Persistent Threats (see References for its relationship to the current NIST publication cited in the Introduction).

Definitional/historical synthesis traces cyber resilience's conceptual lineage from ecological and engineering resilience (Linkov & Kott, 2018). Comparative surveys evaluate frameworks, strategies, and tools (Sepúlveda-Estay et al., 2020). Sector- and standard-mapping empirical studies cover Industrial IoT gaps against NIST CSF (Axon et al., 2021), human-factors practices (Rohan et al., 2023), Philippine SME adoption, and Norwegian OT control deployment. SME-focused maturity/operationalization models appear in Carías et al. (2020a/b), and comprehensive business-oriented models covering governance through recovery in Kanaan et al. and AL-Hawamleh.

Further strands include human/behavioral dimensions (Kleij & Leukfeldt, 2020), sector-specific conceptual work spanning finance, insurance, and societal actors (Dupont, 2019; Hausken, 2020; Safitra et al., 2023 — see Section 5.2), and technical contributions including a CPS experimentation platform (Thorpe et al., 2022), autonomous mission-aware resiliency agents (Gkoktsis et al., 2022), a blockchain/federated-learning zero-trust architecture, a citizen-level resilience ontology (Thinyane & Christine, 2020), and a validated Cyber-Resilience Index for a real 4GW virtual power plant deployment — one of the few studies validated against real operational data rather than simulation.

Material and Methods

Search strategy and databases

Records were identified through three databases: IEEE Xplore, ACM Digital Library, and Google Scholar. Scopus and Web of Science were **not searched**, because neither is accessible without institutional login; this is treated as a limitation of coverage (Section 5.4), not an oversight.

Boolean search strings combined a mandatory cyber-domain anchor ("cyber resilien*" *OR "digital resilience" OR "cyber resiliency") with phase-specific term clusters for Anticipate, Withstand, and Recover, plus a Framework cluster (NIST CSF, ISO 27001, ISO 22301, MITRE CREF). The process differed by database:*

- **IEEE Xplore.** Fourteen CSV exports (918 raw rows) were deduplicated by DOI (falling back to normalized title + year), removing 38 duplicates and leaving 880 unique records. One search string that initially omitted the cyber-domain anchor produced an anomalous 2,391 off-topic hits (e.g., earthquake early-warning, radar clutter suppression) and was corrected before the final export set was used.
- **ACM Digital Library.** ACM's search interface blocks automated access (robots.txt), so the Crossref DOI-registry API (filtered to ACM's 10.1145 prefix) yielded 31 candidate records, and direct manual searching yielded 49 full-text PDFs; after

removing 4 overlaps/duplicates, this contributed 45 additional unique records with full text already in hand.

- **Google Scholar.** Also searched manually (automated querying is against its terms of service), yielding 25 full-text PDFs, of which 2 were removed (1 duplicate, 1 off-topic), leaving 23 new unique records.

This produced **980 unique records** (880 IEEE + 31 ACM-via-Crossref + 45 ACM-direct + 23 Google Scholar, net of one cross-database duplicate). Reconciled against total raw volume actually exported/downloaded (1,023 records: 918 IEEE + 80 ACM + 25 Google Scholar), 43 duplicates were removed across the three databases (IEEE 38, ACM 4, Google Scholar 1). This 1,023/43/980 accounting — rather than the Search Log's raw per-query hit sum of 2,551, which double-counts overlapping search strings — is the basis for the PRISMA flow diagram (Figure 1). The evidence base is confirmed finalized; no further searches or retrieval are planned.

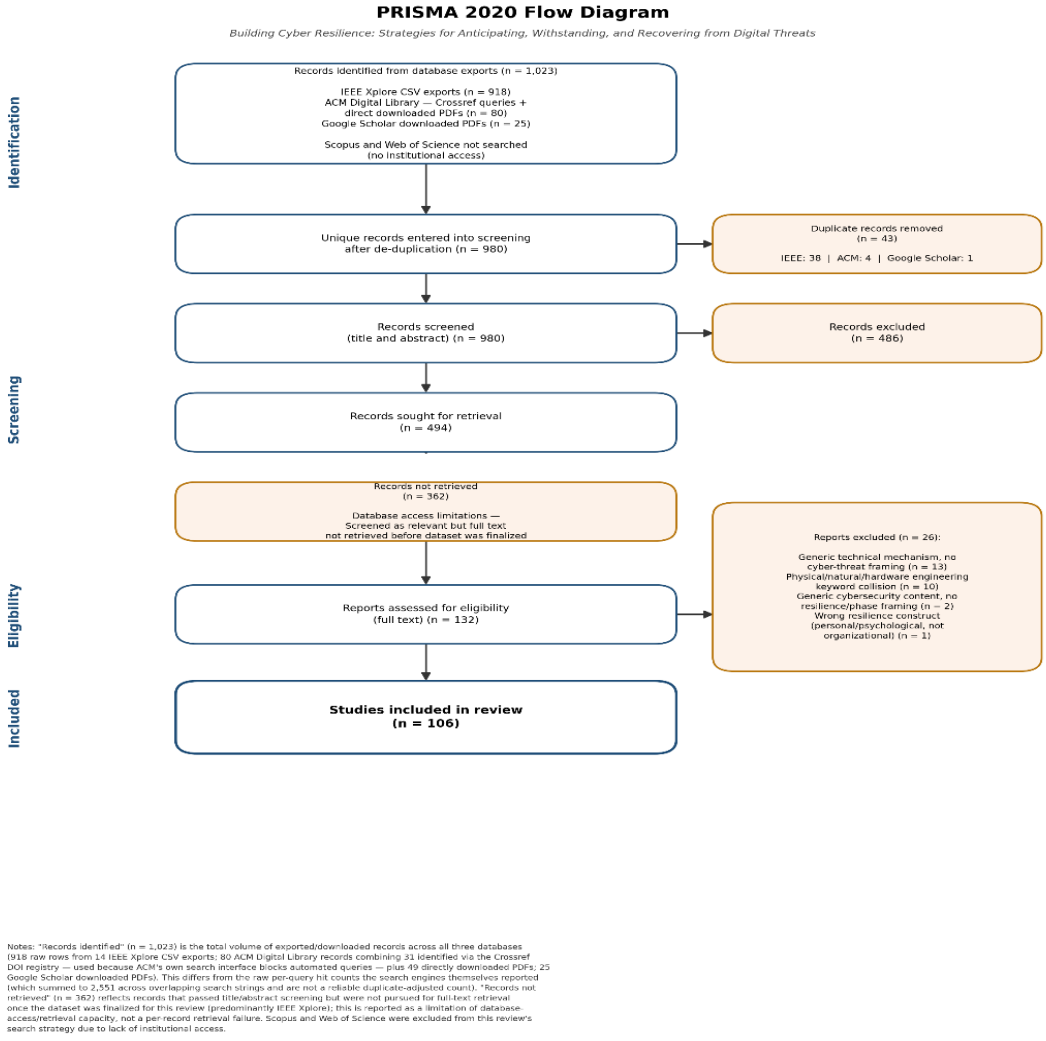

Figure 1. PRISMA 2020 flow diagram of the identification, screening, eligibility, and inclusion process.

Screening and eligibility

Title/abstract screening applied the inclusion criterion that a study concerns organizational or technical cyber-threat resilience mapped to the three-phase model, excluding non-cyber uses of "resilience" (ecological, structural/seismic, psychological, medical-device physical reliability), generic fault-tolerance/database-recovery mechanisms

with no cyber-threat framing, wrong publication types, and keyword false-positives (e.g., "security" matching inside "insecurity").

486 records were excluded at screening; **494 passed**. Of these, **132** (IEEE 46, ACM-direct 38, ACM-via-Crossref 25, Google Scholar 23) had full text retrieved and were assessed for eligibility; **362 passed screening but were never retrieved** as full text before the evidence base was finalized — a database-access/retrieval-capacity limitation (Section 5.4), not a per-record failure. Of the 132 assessed, **26 were excluded at eligibility** (IEEE 17, ACM-direct 6, ACM-via-Crossref 3): 13 were generic technical mechanisms without cyber-threat framing, 10 were physical/hardware-engineering papers matching keywords in an unrelated domain, 2 were generic cybersecurity papers without phase-specific framing, and 1 used "digital resilience" to mean personal wellbeing. **106 studies were included** (Section 2; Figure 1).

A methodological caveat bears on how the 362 unretrieved records should be read: when a batch of 68 full texts was reviewed completely, 20 (29%) turned out to be false positives despite passing title/abstract screening — natural-hazard, military, or hardware papers matching resilience vocabulary in unrelated domains — compared with 6 of an earlier 64 (9%). A comparable rate likely applies to the unretrieved 362, so the true number of additional eligible studies among them is almost certainly smaller than 362; this review does not claim otherwise.

Data extraction

For each of the 106 included studies, the full PDF was read to extract authors, country/organizational context, method, phase focus, research type, and key findings; fields not explicitly stated are marked "Not stated in paper" rather than inferred, and partial reads (e.g., long surveys, slide-deck-style presentations) are flagged in the underlying data-extraction record.

Four author/year combinations recur across different papers and are disambiguated with letter suffixes: Bodeau et al. (2014a/b), Mooi & Botha (2016a/b), Khou et al. (2017a/b), and Carías et al. (2020a/b); Ross et al. is disambiguated by year alone (2019/2021 — see References).

Results and Discussion

Table 2
Research type distribution across the 106 included studies.

Research type	Count
Framework/model proposal	33
Simulation/technical evaluation	23
Systematic/literature review	14
Conceptual/theoretical	13
Case study	8
Empirical (qualitative)	6
Empirical (mixed methods)	5
Empirical (quantitative)	4

Framework/model proposals and simulation/technical evaluations together account for **56 of 106 studies (53%)**, with a further 14 systematic reviews and 13 conceptual papers. Genuinely empirical work with primary organizational data accounts for only **15 of 106 studies (14%)**, plus 8 case studies (several explicitly preliminary — e.g., Davies & Patel, 2016). The evidence base leans toward proposing and technically evaluating mechanisms rather than empirically observing how organizations actually anticipate, withstand, or recover from cyber threats in practice.

- **Post-incident crisis communication** is a narrow but real gap: none of the 106 studies treats communication with stakeholders, media, or customers after an incident as its primary focus.
- **Empirical evidence remains thin relative to frameworks and simulations**; several included case studies are explicitly preliminary (Davies & Patel, 2016).
- **Geographic concentration has broadened but remains uneven.** Real examples span South Africa, Pakistan, Peru, Kuwait, Ukraine, South Korea, Finland, Japan, Brazil, Germany, and Canada, but US-, UK-, and Germany-affiliated authorship remains the largest cluster, and Latin America (beyond Peru/Brazil) and Sub-Saharan Africa (beyond South Africa) remain thin — an observed pattern in this sample, not a claim about the global literature.
- **Sector concentration persists** in smart grid/critical infrastructure, SCADA/ICS, government CSIRTs, and SMEs; healthcare gained one genuine data point (Acharya et al., 2015, with a HIPAA-compliance finding) but remains thin relative to its real-world importance as an attack target.

Conclusion

The 106 included studies show that cyber-resilience maturity differs meaningfully by phase. **Anticipate is the most mature and technically saturated**, dominated by cyber threat intelligence (its production, correlation, attribution, and organizational sharing) and situational awareness (technical monitoring architectures and the human/organizational side of maintaining it). A smaller family addresses risk/vulnerability assessment against recognized standards. Two tensions are worth stating: most of this literature represents a decade or more of continuous technical refinement (2013–2025) without a correspondingly mature body of evidence that better CTI or situational awareness actually translates into fewer or shorter incidents — the causal link is largely assumed rather than measured; and several foundational papers (e.g., Settanni et al., 2016; Ahrend et al., 2016; Kim et al., 2016) are now roughly a decade old, while the threat landscape (ransomware-as-a-service, AI-enabled attacks) has changed substantially.

Withstand is comparatively thin and fragmented: no single strategy dominates the way CTI dominates Anticipate. Studies cluster loosely around Zero Trust architectures, CPS-specific detection/mitigation mechanisms that are often domain-specific rather than generalizable, and a smaller set of engineering approaches to building resilience directly into system design (Wheeler, 2019; Troiani, 2020; Khan et al., 2015). This fragmentation is itself a finding: the literature has not converged on a small number of well-validated Withstand strategies.

Recover has changed substantially since an earlier interim analysis of this evidence base, splitting into two mature technical strands (ransomware detection/recovery, disaster-recovery/backup architecture) and one genuinely organizational strand — CSIRT establishment, management, and evaluation (Mooi & Botha, 2016a/b; Tariq et al., 2013; Kassim et al., 2023) describing how organizations and even national bodies build institutional recovery capability, which is precisely the organizational-strategy evidence RQ1 asks about. Several of the newest technical Recover contributions (Ma et al., 2023) are recent single-study proposals without independent replication in this evidence base, so their generalizability should not be overstated.

Cross-cutting theme: Adaptation

Several included studies explicitly invoke a fourth concept — Adapt/Adaptation/Evolve — that does not fit cleanly into any single phase and is treated here as a cross-cutting theme rather than a fourth category. The clearest anchor is the MITRE CREF lineage itself: Bodeau & Graubart (2011) and its updates define cyber

resiliency around four goals — Anticipate, Withstand, Recover, and Evolve — with Evolve concerned with changing missions, threats, and technologies over time. Thinyane & Christine (2020) build "adapt" into their citizen-level SC2R ontology; Gkoktsis et al. adopt the same four-part NIST/MITRE definition for their Cyber-Resilience Index — the same definition this review's Introduction draws on directly. Beyond the CREF lineage, Safitra et al. (2023) frame an "adaptive cybersecurity mindset" as a necessary organizational orientation, and Babar et al. operationalize adaptation technically — their reinforcement-learning agents dynamically adapt detection thresholds to changing attack conditions.

Reading across these, Adaptation operates at three levels that should not be conflated: **strategic/organizational** (mission or posture evolving over time — Safitra et al., 2023; the CREF "Evolve" goal), **architectural** (a system's own structure or parameters changing dynamically), and **individual/citizen-level** (Thinyane & Christine, 2020, a notably different unit of analysis). The evidence for Adaptation is real but thin relative to the three core phases — an under-theorized fourth dimension in the literature actually retrieved, stated here as a genuine finding rather than papered over.

Framework/model proposals and simulation/technical evaluations together account for 53% of included studies, while genuinely empirical organizational research accounts for only 14%. Read alongside the phase-level findings above, this suggests a specific gap: the field is good at proposing mechanisms and increasingly good at technically validating narrow ones, but comparatively weak at empirically studying how real organizations — beyond the single-organization case studies reported as preliminary (Davies & Patel, 2016) — actually implement or sustain any of these strategies over time.

Limitations

This review's limitations are stated plainly rather than smoothed into generic boilerplate.

1. **Database coverage.** Scopus and Web of Science were not searched because institutional access was not available — a material limitation, since both index cybersecurity and management literature not necessarily covered by IEEE Xplore, ACM Digital Library, or Google Scholar.

2. **Incomplete retrieval, with an evidenced quality caveat.** Of the 494 records that passed screening, only 132 (27%) were retrieved and assessed before the evidence base was finalized; 362 were never retrieved. This review does not assume the missing 362 would contribute proportionally more included studies — a reviewed batch of 68 full texts showed a 29% false-positive rate despite passing automated screening, so a meaningful share of the 362 would likely not have been eligible even if retrieved, though this cannot be confirmed without doing so.

3. **Screening and full-text/extraction judgment were not independently dual-reviewed** — a departure from PRISMA best practice. The classifier's own measured error rate (29% on one batch, 9% on an earlier batch) is reported precisely because its stated counts should not be taken as more reliable than that.

4. **Extraction depth was uneven** for some studies — long surveys, slide-deck-style presentations (Bodeau, 2018; Wheeler, 2019; Troiani, 2020), and papers presenting only preliminary results (Davies & Patel, 2016) — relying on partial reads of the most resilience-relevant sections.

5. **Empirical evidence is thin and skews technical**: only 14% of included studies are empirical organizational research (Sections 4.1, 5.3).

6. **Geographic and sector concentration** persists despite meaningfully broad representation: US-, UK-, and Germany-affiliated authorship remains the largest cluster, and several regions/sectors (healthcare beyond one study, most of Latin America and Sub-Saharan Africa) remain thin.

7. **Currency.** A meaningful share of the Anticipate/Withstand literature predates 2020, while the threat landscape it addresses has continued to evolve; findings from this older literature should not be read as reflecting current conditions.

Concluding synthesis

This review synthesized 106 studies from IEEE Xplore, ACM Digital Library, and Google Scholar (Scopus and Web of Science were inaccessible) to characterize how organizations build cyber resilience across Anticipate, Withstand, and Recover, with Adaptation as a cross-cutting fourth theme. Maturity is uneven by phase — Anticipate is most developed, Withstand is fragmented, and Recover is now substantively represented but still light on post-incident crisis communication — while Adaptation remains a real but under-theorized fourth dimension. Methodologically, the field leans heavily toward framework/model proposals and simulation/technical evaluations (53% combined), with genuinely empirical organizational research accounting for only 14%.

Given the limitations detailed in Section 5.4 — absent Scopus/Web of Science coverage, 362 screened-but-unretrieved records, and single-reviewer screening and extraction — these conclusions should be read as a rigorous synthesis of a bounded, transparently documented evidence base rather than an exhaustive census of the cyber-resilience literature.

Recommendation

Three gaps stand out as most actionable, in descending order of evidentiary support: (1) **post-incident crisis communication** — despite substantial CSIRT-process coverage, no included study treats stakeholder/media/customer communication after an incident as its primary focus; (2) **empirical validation of Withstand- and Recover-phase technical mechanisms** beyond their originating authors' own testbeds — most of the newest technical contributions report strong single-setup results with no independent replication; and (3) **the relationship between Adaptation and the three core phases**, which remains under-theorized — several studies gesture at it but none empirically studies how organizations adapt their posture over time.

References

Acharya, S., Glenn, W., & Carr, M. (2015, November). A GRReat framework for incident response in healthcare. In *2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)* (pp. 776-778). IEEE.

Ahrend, J. M., Jirotka, M., & Jones, K. (2016, June). On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. In *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)* (pp. 1-10). IEEE.

Al-Enezi, K. A., Al-shaikhli, I. F., Al-kandari, A. R., & Al-Mutairi, H. M. (2013, December). E-business Continuity and Disaster Recovery Plan Case Study Kuwait: Kuwait Government Entities (GEs). In *2013 International Conference on Advanced Computer Science Applications and Technologies* (pp. 504-509). IEEE.

AlKilani, H., & Qusef, A. (2021, April). OSINT techniques integration with risk assessment ISO/IEC 27001. In *International Conference on Data Science, E-learning and Information Systems 2021* (pp. 82-86).

Allison, D., Smith, P., & Mclaughlin, K. (2023, August). Digital twin-enhanced incident response for cyber-physical systems. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-10).

Annarelli, A., & Palombi, G. (2021). Digitalization capabilities for sustainable cyber resilience: A conceptual framework. *Sustainability*, *13*(23), 13065.

Axon, L., Fletcher, K., Scott, A. S., Stolz, M., Hannigan, R., Kaafarani, A. E., ... & Creese, S. (2022). Emerging cybersecurity capability gaps in the industrial internet of things: Overview and research agenda. *Digital Threats: Research and Practice*, *3*(4), 1-27.

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of cyber policy*, *3*(2), 258-283.

Bajpai, P., & Enbody, R. (2023). Know thy ransomware response: a detailed framework for devising effective ransomware response strategies. *Digital Threats: Research and Practice*, *4*(4), 1-19.

Barrere, M., Badonnel, R., & Festor, O. (2013). Vulnerability assessment in autonomic networks and services: A survey. *IEEE communications surveys & tutorials*, *16*(2), 988-1004.

Bodeau, D. J., Graubart, R., Picciotto, J., & McQuaid, R. (2011). Cyber resiliency engineering framework.

Bodeau, D., Graubart, R., Heinbockel, W., & Laderman, E. (2015). Cyber resiliency engineering aid-the updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques.

Bodeau, D., Brtis, J., Graubart, R., & Salwen, J. (2014, August). Resiliency techniques for systems-of-systems extending and applying the Cyber Resiliency Engineering Framework to the space domain. In *2014 7th International Symposium on Resilient Control Systems (ISRCS)* (pp. 1-6). IEEE.

Bodeau, D. (2019). Cyber Resiliency Overview: What Is It, and How Do We Build It into Our Systems?. *ACM SIGAda Ada Letters*, *38*(2), 58-63.

Burton, J. (2016, June). Cyber attacks and maritime situational awareness evidence from Japan and Taiwan. In *2016 International Conference on Cyber Situational Awareness, Data analytics and Assessment (CyberSA)* (pp. 1-4). IEEE.

Cam, H., & Mouallem, P. (2013, January). Mission-aware time-dependent cyber asset criticality and resilience. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop* (pp. 1-4).

Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber resilience progression model. *Applied Sciences*, *10*(21), 7393.

Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE access*, *8*, 174200-174221.

Cassottana, B., Roomi, M. M., Mashima, D., & Sansavini, G. (2023). Resilience analysis of cyber-physical systems: A review of models and methods. *Risk Analysis*, *43*(11), 2359-2379.

Chen, C. M., Hsu, F. H., & Hwang, J. N. (2023, June). Useful cyber threat intelligence relation retrieval using transfer learning. In *Proceedings of the 2023 European interdisciplinary cybersecurity conference* (pp. 42-46).

Cho, H., Lee, S., Kim, B., & Lee, T. (2016, July). The data indexing for cyber threat resources. In *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 1059-1061). IEEE.

Davies, M., & Patel, M. (2016, June). Are we managing the risk of sharing cyber situational awareness? A UK Public Sector case study. In *2016 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-2). IEEE.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

Eke, H., Petrovski, A., & Ahriz, H. (2020, November). Detection of false command and response injection attacks for cyber physical systems security and resilience. In *13th International Conference on Security of Information and Networks* (pp. 1-8).

Gabriel, A., Shi, J., & Ozansoy, C. (2017). A proposed alignment of the national institute of standards and technology framework with the funnel risk graph method. *IEEE Access*, *5*, 12103-12113.

Gizun, A., Gnatyuk, V., Balyk, N., & Falat, P. (2015). Approaches to improve the activity of computer incident response teams. *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 442–447.

Gkoktsis, G., Lauer, H., & Jäger, L. (2023). Towards Mission Aware Cyber-Resiliency with Autonomous Agents. In *Proceedings of the 2023 Australasian Computer Science Week* (pp. 36-39).

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204.

He, Y., Maglaras, L. A., Janicke, H., & Jones, K. (2015, September). An industrial control systems incident response decision framework. In *2015 IEEE Conference on Communications and Network Security (CNS)* (pp. 761-762). IEEE.

Ibne Hossain, N. U., Nagahi, M., Jaradat, R., Shah, C., Buchanan, R., & Hamilton, M. (2020). Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem. *Journal of Computational Design and Engineering*, *7*(3), 352-366.

Mohd Kassim, S. R. B., Li, S., & Arief, B. (2023). Understanding how national CSIRTs evaluate cyber incident response tools and data: Findings from focus group discussions. *Digital Threats: Research and Practice*, *4*(3), 1-24.

Khan, Y. I., Al-Shaer, E., & Rauf, U. (2015, October). Cyber resilience-by-construction: Modeling, measuring & verifying. In *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense* (pp. 9-14).

Khou, S., Mailloux, L. O., Pecarina, J. M., & Mcevilley, M. (2017). A customizable framework for prioritizing systems security engineering processes, activities, and tasks. *IEEE access*, *5*, 12878-12894.

Khou, S., Mailloux, L. O., & Pecarina, J. M. (2017). System-agnostic security domains for understanding and prioritizing systems security engineering efforts. *IEEE Access*, *5*, 3465-3474.

Kim, D., Woo, J., & Kim, H. K. (2016, November). "I know what you did before": General framework for correlation analysis of cyber threat incidents. In *MILCOM 2016-2016 IEEE Military Communications Conference* (pp. 782-787). IEEE.

van der Kleij, R., & Leukfeldt, R. (2019, June). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. In *International conference on applied human factors and ergonomics* (pp. 16-27). Cham: Springer International Publishing.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks* (pp. 1-25). Springer, Cham.

Ma, B., Yang, Y., Li, J., Zhang, F., Shen, W., Zhou, Y., & Ma, J. (2023, November). Travelling the hypervisor and ssd: A tag-based approach against crypto ransomware with fine-grained data recovery. In *Proceedings of the 2023 ACM SIGSAC conference on computer and communications security* (pp. 341-355).

Mavroeidis, V., & Bromander, S. (2017, September). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)* (pp. 91-98). IEEE.

Jezreel, M., Mirna, M., & Edgar, U. (2015, June). Services establishment in the computer security incident response teams: A review of state of art. In *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

Mepham, K., Louvieris, P., Ghinea, G., & Clewley, N. (2014, June). Dynamic cyber-incident response. In *2014 6th International conference on cyber conflict (CyCon 2014)* (pp. 121-136). IEEE.

Mooi, R. D., & Botha, R. A. (2016). A management model for building a computer security incident response capability. *SAIEE Africa Research Journal*, *107*(2), 78-91.

Mooi, R., & Botha, R. A. (2016, May). Context for the SA NREN Computer Security Incident Response Team. In *2016 IST-Africa Week Conference* (pp. 1-9). IEEE.

Nafees, M. N., Saxena, N., & Burnap, P. (2021, November). Optimized predictive control for AGC cyber resiliency. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2450-2452).

Nguyen, D. T., Shen, Y., & Thai, M. T. (2013). Detecting critical nodes in interdependent power networks for vulnerability assessment. *IEEE Transactions on Smart Grid*, *4*(1), 151-159.

Nykänen, R., & Kärkkäinen, T. (2016, August). Supporting cyber resilience with semantic wiki. In *Proceedings of the 12th International Symposium on Open Collaboration* (pp. 1-8).

Padayachee, K., & Worku, E. (2017, December). Shared situational awareness in information security incident management. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 479-483). IEEE.

Porter, C., Khan, S., & Pande, S. (2023, January). Decker: Attack surface reduction via on-demand code mapping. In *Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2* (pp. 192-206).

Rebah, H. B., & Sta, H. B. (2016, July). Disaster recovery as a service: A disaster recovery plan in the cloud for SMEs. In *2016 Global Summit on Computer & Information Technology (GSCIT)* (pp. 32-37). IEEE.

Rohan, R., Papasratorn, B., Chutimaskul, W., Hautamäki, J., Funilkul, S., & Pal, D. (2023, December). Enhancing cybersecurity resilience: A comprehensive analysis of human factors and security practices aligned with the NIST cybersecurity framework. In *Proceedings of the 13th International Conference on Advances in Information Technology* (pp. 1-16).

Rommel, F., Dietrich, C., Ziegler, A., Ostapyshyn, I., & Lohmann, D. (2023, June). Thread-level attack-surface reduction. In *Proceedings of the 24th ACM SIGPLAN/SIGBED International Conference on Languages, Compilers, and Tools for Embedded Systems* (pp. 64-75).

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). *Developing cyber resilient systems: a systems security engineering approach* (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft)). National Institute of Standards and Technology.

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.

Estay, D. A. S., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & security*, *97*, 101996.

Settanni, G., Shovgenya, Y., Skopik, F., Graf, R., Wurzenberger, M., & Fiedler, R. (2016, December). Correlating cyber incident information to establish situational awareness in Critical Infrastructures. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 78-81). IEEE.

Shovgenya, Y., Skopik, F., & Theuerkauf, K. (2015, June). On demand for situational awareness for preventing attacks on the smart grid. In *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-4). IEEE.

Shreeve, B., Hallett, J., Edwards, M., Anthonysamy, P., Frey, S., & Rashid, A. (2020). "So If Mr Blue Head Here Clicks the Link..." risk thinking in cyber security decision making. *ACM Transactions on Privacy and Security (TOPS)*, *24*(1), 1-29.

da Silva, M. P., & de Barros, R. M. (2017). Maturity model of information security for software developers. *IEEE Latin America Transactions*, *15*(10), 1994-1999.

Singhal, M. K. (2022, December). Protecting customer databases to shield business data against ransomware attacks and effective disaster recovery in a hybrid production environment. In *Proceedings of the 4th International Conference on Information Management & Machine Intelligence* (pp. 1-5).

Takano, M. (2014, September). ICS cybersecurity incident response and the troubleshooting process. In *2014 Proceedings of the SICE Annual Conference (SICE)* (pp. 827-832). IEEE.

Tariq, M., Aslam, B., Rashid, I., & Waqar, A. (2013, December). Cyber threats and incident response capability-a case study of Pakistan. In *2013 2nd National Conference on Information Assurance (NCIA)* (pp. 15-20). IEEE.

Thinyane, M., & Christine, D. (2020, November). SMART citizen cyber resilience (SC2R) ontology. In *13th International Conference on Security of Information and Networks* (pp. 1-8).

Thorpe, J., Fasano, R., Galiardi Sahakian, M., Gonzales, A., Hahn, A., Morris, J., ... & Vugrin, E. D. (2022, April). A cyber-physical experimentation platform for resilience analysis. In *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems* (pp. 3-12).

Timonen, J. (2015, June). Improving situational awareness of cyber physical systems based on operator's goals. In *2015 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-6). IEEE.

Troiani, M. (2020). Ensuring Cyber Resilience through Entropy-Augmented Replication. *ACM SIGAda Ada Letters*, *39*(1), 72-72.

Tupia, M., Bruzza, M., & Rodriguez, F. (2016, September). An information security framework for ubiquitous services in e-government structures: a peruvian local government experience. In *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)* (pp. 1309-1316). IEEE.

Wheeler, D. A. (2019). Approaches to Cyber-Resilience through Language System Design. *ACM SIGAda Ada Letters*, *38*(2), 43-57.