

DOI: https://doi.org/10.48009/4_iis_2026_107

When everything is critical, nothing is: Risk-based prioritization and cyber resilience in practice

Dr. Brian Massa, *Robert Morris University*, brianmassa1987@gmail.com

Dr. A. J. Grant, *Robert Morris University*, granta@rmu.edu

Abstract

Cyber resilience has emerged as a strategic necessity for organizations navigating a relentless and ever-evolving threat landscape. This qualitative study, which forms the basis of this paper, investigated the primary research question: how organizations understand and apply cyber resilience tools, techniques, and practices to combat these threats. Drawing on semi-structured interviews with 27 information security professionals across the public, private, and non-profit sectors, data was analyzed using an iterative data spiral and pattern-matching analysis. The findings reveal a fundamental philosophical shift toward an “assumed compromise” mindset that prioritizes recovery and continuity over mere prevention. A central finding is that risk-based prioritization, grounded in the disciplined identification of critical assets, serves as the operational foundation upon which all other resilience capabilities depend. Participants observed that when organizations treat everything as critical, nothing is, further noting that while artificial intelligence and machine learning are positioned as essential force multipliers for managing modern data volumes, their effective application is fundamentally sabotaged by a persistent human-knowledge gap and the lack of a shared organizational lexicon. The study concludes that genuine cyber resilience is not merely a technical outcome but emerges from the disciplined integration of people, processes, and technology, anchored in risk-based asset management.

Keywords: cyber resilience, cybersecurity, risk-based prioritization, artificial intelligence and machine learning, human-knowledge gap, practitioner insights

Introduction

Cyberspace is a global domain within the information environment that comprises an interdependent network of information security infrastructures, including telecommunication networks, computer systems, embedded processors, and controllers (NIST, 2023, pp. 5–8, 17–22; NIST CSRC, 2024). The omnipresence of cyber threats has led to the exploitation and manipulation of critical personal and private information (Akcadag, 2012, pp. 1–4; Djenna et al., 2021, pp. 2–6). The security market is flooded with a myriad of options, from endpoint systems to Software-as-a-Service. It is very challenging for organizations to determine the best way to protect their data and systems.

This global domain of cyberspace is where the new frontier of warfare is being conducted. This is the only domain in which private citizens and the military share the same battlespace (Cains et al., 2022). It is in this battlespace that organizations are trying to protect their information assets while conducting business simultaneously. It is in this uniquely complex and demanding environment that organizations operate.

Organizations overemphasize preventive controls while under-integrating pre- and post-event cyber resilience within comprehensive strategies. The most common frameworks used in cyber organizations focus on risk management or on preventing breaches. Examining the cyber data from current reports, it is evident that systems continue to be exploited. Different types of malware emerge every year, yet organizations continue to remain vulnerable to cyberattacks (Symantec, 2019; Symantec, 2023). Pearlson (2024) recently surveyed 30 cyber executives, who believed that protection was sufficient for cyber-resiliency but did not focus enough on recovery, instead relying on business continuity plans that were not designed for cyber incidents.

This study addressed how practitioners understand and apply cyber resilience tools, techniques, and practices in this environment, with particular attention to the role of emerging AI and machine learning capabilities. The research question guiding the study was: how do organizations understand and apply cyber resilience tools, techniques, and practices to combat evolving threats? Semi-structured interviews were conducted with 27 information security professionals across the public, private, and non-profit sectors. Four of the nine themes that emerged from the study inform the analysis presented in this paper: Understanding and Defining Cyber Resilience; Tools, Technologies, and Data Analysis; Threats, Risks, and Vulnerabilities; and Implementation Challenges and Obstacles.

These four themes were selected because they most directly address the central inquiry of how practitioners understand and apply cyber resilience tools, techniques, and practices (RQ1). Themes 1, 4, and 5 map primarily to RQ1 and examine, respectively, how cyber resilience is conceptualized, the specific technologies practitioners deploy, and the threat environment that shapes those decisions. Theme 7 (Implementation Challenges and Obstacles), while also relevant to RQ2 and RQ3 addressed in companion papers, is included because implementation barriers (particularly tool redundancy, framework complexity, and workforce limitations) directly constrain how resilience practices are applied in organizational settings. The four themes retain their original numbering (1, 4, 5, and 7) from the nine-theme structure of the parent study, so that readers can trace them directly to the dissertation. Together, they trace an arc from definitional clarity through tool deployment, threat context, and implementation realities, forming a coherent analytical lens on the research question.

The remainder of this paper is organized as follows. The Background and Literature Review summarizes cyber resilience theory, the landscape of frameworks, and emerging research on AI in cyber operations. The Research Question section states the question this paper addresses. The Methodology describes the qualitative design. The Results and Findings section presents the four themes that informed the analysis. The Discussion of Findings interprets the results in light of the literature. The paper then presents the study's principal contributions before closing with implications, limitations, and conclusions.

Background and Literature Review

This section reviews the foundations of cyber resilience theory and the relevant framework landscape for applying resilience tools, techniques, and practices in organizations, with particular attention to the human side of resilience and the role of emerging artificial intelligence and machine learning capabilities.

The Evolution of Cyberspace

In 1957, the Advanced Research Projects Agency (ARPA) was created to help the United States fight the Soviet Union's perceived technological advantage. Early studies within ARPA revealed the potential devastation of a nuclear attack and the crippling effects that the blast would have on communications infrastructure (Pool, 2013). ARPA's response was to create a communications system in which, if one node

went down, traffic could be rerouted through the interconnected nodes. These nodes created by ARPA would serve as the foundation for the decentralized internet model known today. In 1988, Robert Morris, a Cornell student, released the first attributed piece of malware, known as the Morris worm. This malware paved the way for the vulnerabilities in the wild today (Morgan, 2016). The cyber threat has evolved from a 1988 worm that affected 600 computers into a pervasive, relentless, and ever-evolving threat landscape.

Cyber Resilience Theory

Cyber resiliency theory exposes the gaps in traditional cybersecurity thinking. When cybersecurity was established as a discipline, systems were not designed with resiliency in mind. When ARPA was created and TCP/IP was implemented (Pool, 2013), the inventors prioritized a system's functionality over security. The world has undergone significant changes with the advent of internet connectivity and an abundance of online information, and cybersecurity threats are more severe than ever. This is why cyber-resiliency should be one of the pillars that organizations focus on; yet it is lacking in both practice and research.

The Cyber Resiliency Engineering Framework

The Cyber Resiliency Engineering Framework (CREF) was developed by the MITRE Corporation to address cyber-resiliency goals on behalf of the U.S. Government, aiming to address critical cyber-resiliency shortfalls observed in organizations implementing effective cyber-resiliency measures (Bodeau & Graubart, 2011). Bodeau and Graubart (2011) define the framework's four goals as: "Anticipate: maintain a state of informed preparedness to forestall compromises of mission functions from adversary attacks"; "Withstand: continue essential mission functions despite the successful execution of an attack by an adversary"; "Recover: restore mission functions to the maximum extent possible after the successful implementation of an attack by an adversary"; and "Evolve: to change mission functions and the supporting cyber capabilities to minimize adverse impacts from actual or predicted adversary attacks" (pp. 14–17). "Reaching these goals requires achieving cyber-resiliency objectives: understand, prepare, prevent, constrain, continue, reconstitute, transform, and re-architect" (Bodeau & Graubart, 2011, p. iii). CREF was created with the military in mind, but is highly applicable to the civilian world.

The Cyber Preparedness Methodology

Bodeau et al. (2010) developed the Cyber Preparedness Methodology (CPM) to classify cyber threats and determine the level of preparedness appropriate for a particular organization. The CPM enables an organization to "(a) characterize the cyber threats faced by an organization or mission, (b) determine the cyber preparedness level necessary to ensure mission success, (c) facilitate strategic planning for cybersecurity (CS) by setting preparedness objectives, and (d) establish priorities for CS investment planning and management decisions" (Bodeau et al., 2010, pp. 1147–1149). The CPM defines five cyber preparedness levels: Foundational Defense, Critical Information Protection, Responsive Awareness, Architectural Resilience, and Pervasive Agility (Bodeau & Graubart, 2011, p. 3). Each preparedness level builds on the defenses and activities an organization has implemented to prepare for lower-level threats.

NIST 800-160 Volume 2

The National Institute of Standards and Technology issued Special Publication 800-160, Volume 2 (Developing Cyber-Resilient Systems: A Systems Security Engineering Approach) to guide organizations in embedding resilience principles into system design and engineering practices. This publication categorizes the MITRE CREF framework, codifying cyber resilience to augment the NIST CSF, NIST 800-53, and NIST 800-171, specifically addressing controls related to the Risk Management Framework (Ross et al., 2019; NIST, 2023). NIST 800-160 v2 introduces the foundational assumption that the adversary "will compromise or breach the system or organization" (NIST, 2023, pp. 123–129), a premise that distinguishes the framework from traditional preventive cybersecurity guidance.

Frameworks and Standards in Practice

Cybersecurity standards are generally classified into two main categories: information security standards (e.g., the ISO/IEC 27000 series, NIST 800 series) and information security governance standards (e.g., COBIT, NIST CSF) (Taherdoost, 2022). The ISO/IEC 27000 series, originating as the British Standard for Information Security Management (BS 7799), focuses on information security management systems and risk management. The NIST Cybersecurity Framework (CSF) was developed following Executive Order 13636 and the Cybersecurity Enhancement Act of 2014, which formalized NIST's role in developing cybersecurity risk frameworks for critical infrastructure operators. COBIT, developed by ISACA in 1996, focuses on IT governance and control objectives. NIST 800-53, NIST 800-171, the Cybersecurity Capability Maturity Model (C2M2), and the Center for Internet Security (CIS) controls round out the most commonly cited frameworks in practitioner settings (Watson, 2019). According to a U.S. survey by Vanson Bourne, only 30% of organizations had adopted a cyber-resiliency strategy at the time of the survey (Gardner, 2019).

Risk Versus Resilience

In critical infrastructure and services, resilience is defined by four key abilities: planning and preparation for, absorbing, recovering from, and adapting to known and unknown threats (Mylrea, 2018, pp. 34-38). Current methods of promoting cyber resilience often conflict with resilience and risk, where risk is defined as the product of the likelihood of an adverse event and the magnitude of the resulting damage. Executive Order 13636 directed the development of risk-based standards to protect critical infrastructure against cyber threats; however, risk-based approaches do not necessarily ensure resilience. As Mylrea (2018) observed, "change theory about how to transform an organization's policies and processes to become more resilient needs to be in place for organizations to survive threats in an environment of evolving cyber threats" (p. 40). Linkov et al. (2013) further argued that steps must be taken to utilize more generalizable resilience concepts and integrate them with risk-based management approaches.

The Human Side of Cyber Resilience

The human side of cyber resilience is equally critical. Most cybersecurity efforts focus on reducing system vulnerabilities and, to a lesser extent, mitigating the consequences of a successful attack. Rules are often designed with a focus on the computer rather than on the human, which is why cyber-resiliency in the past has not been effective: it has not considered human behavior and the types of behavioral factors that it causes (Gisladdottir et al., 2017). Carias et al. (2020) further observed that cyber resilience can be challenging to operationalize because it is "comprised of several domains (governance, business continuity, information security, etc.) with hundreds of policies within them and intricate relationships between these domains and policies" (pp. 1-2).

Taken together, the cyber resilience literature reflects a field in active development, spanning engineering frameworks, standards-based guidance, organizational behavioral research, and risk management theory. Theoretical contributions range from engineering frameworks (Bodeau & Graubart, 2011) and standards guidance (NIST, 2023; Ross et al., 2019) to organizational and behavioral perspectives on resilience (Carias et al., 2020; Gisladdottir et al., 2017). Empirical studies have examined risk quantification (Linkov et al., 2013), sector-specific implementation (Mylrea, 2018), and practitioner adoption of frameworks (Taherdoost, 2022; Watson, 2019). As a body of work, however, cyber resilience research has remained largely theoretical and framework-focused, with limited empirical investigation of how practitioners actually understand, experience, and apply resilience in organizational settings. The breadth of this literature reflects the multidisciplinary nature of cyber resilience, yet reveals a persistent gap: the practitioner's voice is largely absent from the scholarly conversation.

Research Gap

Much of the existing research focused on critical events in the history of cybersecurity, such as after-action reports, which detail what happened and what can be done to prevent such incidents from happening again. Few studies document how organizations experience and adapt to evolving cyber threats. Empirical data on how organizations protect themselves against attacks is scarce and hard to find. Frameworks can provide organizations with high-level recommendations, but greater specificity is needed to define and apply cyber resilience. As NIST observed, “for the nation to survive and flourish in the 21st century, where hostile actors in cyberspace are assumed, and IT will continue to dominate every aspect of our lives, we must develop trustworthy, secure IT components, services, and systems that are cyber-resilient” (NIST, 2023, p. iv). This study addresses that gap by capturing practitioner perspectives on the understanding and application of cyber resilience tools, techniques, and practices.

Research Question

This paper investigates the following research question: How do organizations understand and apply cyber resilience tools, techniques, and practices to combat evolving threats? The analysis draws on findings from four of the nine themes that emerged from the qualitative study: Understanding and Defining Cyber Resilience; Tools, Technologies, and Data Analysis; Threats, Risks, and Vulnerabilities; and Implementation Challenges and Obstacles.

Methodology

This section describes the qualitative research design, sampling strategy, instrumentation, and analytical approach used to investigate practitioner perspectives on the application of cyber resilience tools, techniques, and practices.

Research Design

This study employed a general qualitative research design with semi-structured interviews as the primary data collection method. The qualitative approach was selected because the research question concerns how practitioners understand and apply cyber resilience, a domain in which meaning is constructed through practitioner experience rather than reducible to quantitative measurement. The study adopted a constructivist epistemological position, defined as “theories of knowledge that emphasize that the world is constructed by human beings as they interact and engage in interpretation” (O’Leary, 2017, p. 7), and a relativist ontological stance consistent with the contextual nature of cybersecurity practice. This stance aligns with cyber research because the discipline is both an art and a skill and lacks universal principles. The semi-structured format aligned with the constructivist paradigm, which assumes that meaning is co-constructed through interaction and that participants’ perspectives are shaped by their professional contexts (Merriam & Tisdell, 2016).

Population and Sample

Participants were information security professionals who met three criteria: at least five years of professional cybersecurity experience; classification at one of three career levels (entry, mid, or senior); and employment in government, private-sector, or non-profit organizations. Recruitment used purposeful sampling combined with maximum variation and critical case sampling to capture diversity across sectors, career levels, and credential profiles (Creswell & Creswell, 2018). Saturation was reached at 27 interviews. Of the 27 participants, 1 (3.7%) was classified as entry-level, 11 (40.7%) as mid-level, and 15 (55.6%) as

senior-level. Six (22.2%) worked exclusively in government, 9 (27%) exclusively in the private sector, and the remainder spanned multiple sectors.

Instrumentation and Data Collection

Semi-structured interviews served as the data collection method. The researcher developed the interview protocol and formulated the interview questions, which appeared in Appendix B of the broader study. A 17-question semi-structured protocol elicited practitioners' perspectives on cyber risk assessment, security incidents, definitions of cyber resilience, organizational strategies, tools and techniques, frameworks, and the perceived impact of AI and autonomous systems on cyber resilience. The interview protocol included open-ended questions appropriate for participants across all levels of organizational seniority.

After receiving Institutional Review Board approval, data collection commenced. Targeted participants were contacted via LinkedIn messages or email, with each message including a brief invitation, the study's purpose, and a formal invitation to participate. The researcher reached out to over 50 candidates. Participants who agreed signed a consent form before scheduling an hour-long, in-person or virtual semi-structured interview. The researcher followed the interview protocol while simultaneously taking field notes and recording the session. Audio recordings were transcribed locally on the researcher's computer using a privacy-preserving transcription tool to prevent data leakage or unauthorized access by third parties. Original recordings were destroyed once transcription accuracy was verified.

Data Analysis

The data was analyzed using Creswell and Poth's (2018) qualitative data analysis spiral, an iterative process of coding, categorizing, and synthesizing information. This approach produced 11 categories and nine themes that reflected how cyber resilience is conceptualized and operationalized in real-world environments. During coding, the frequency with which themes and sub-topics appeared across participants was tracked alongside the interpretive analysis, supporting later observations about the breadth of practitioner discourse on specific topics. Four of those themes most directly informed how organizations understand and apply cyber resilience tools, techniques, and practices, and form the basis of the analysis presented in this paper.

Results and Findings

The following sections present findings from the four themes that informed the analysis of the research question. Each theme is illustrated with representative participant quotations and connected to the relevant literature.

Theme 1: Understanding and Defining Cyber Resilience

Participants described resilience primarily as the ability to recover and maintain normal functioning after a disruption. They recognized that just focusing on prevention was not enough; what mattered was continuing operations even when things went wrong. As Participant 22 explained, cyber resilience “is the ability to display resilience to attacks, to threats, to risks. So, it goes beyond just this defensive mentality and more into how we recover. How do we continue business?” All these dimensions of cyber resilience go beyond the traditional business continuity and disaster recovery paradigms. Participants validated the definition that was outlined in NIST 800-160 v2, which mandates that the adversary “will compromise or breach the system or organization” (NIST, 2023, pp. 123–129).

Although there was a better understanding of what cyber resilience meant, the data revealed that cyber terms were “overloaded...to mean all things to all people” (Participant 21). Participant 27 also stated that

cyber resilience lexicon is a “word salad from an ideology. I just don’t think it’s well defined.” These loaded, confusing terms, coupled with multiple definitions, led to uncertainty about the proper lexicon for defining and conveying what cyber resilience entails. The findings showed that a unified, clear lexicon with standard definitions was crucial for establishing shared expectations and enforceable metrics for cyber resilience.

Theme 4: Tools, Technologies, and Data Analysis

Participants demonstrated technical fluency with the foundational tools used to implement and operate cyber resilience capabilities, including security information and event management (SIEM) platforms such as Splunk, threat modeling, and tactic frameworks such as MITRE ATT&CK, and identity and access management (IAM) as a foundational control. The findings show that participants knew the capabilities and how to employ them, but that this fluency was undermined by the operational difficulties of integrating multiple capabilities simultaneously.

The participants then broadened the findings to specifically address data and the insurmountable, ever-increasing scale of it. Practitioners are increasingly relying on advanced automation, utilizing LLMs and AI or ML capabilities, to sift through logs. This reliance on automation confirms the need to measure “how quickly the threat is detected” (Linkov et al., 2013, p. 471). Participant 11 explained:

Large language models are very helpful for going through your logs and understanding the heuristics of your logs. In addition to that, language translations, Chinese characters, stuff like that, show up in your logs that you might not know are there. AI or ML is great for sifting through all that stuff and building that out.

Participant 2, working in operational technology security, described an active build that combined a digital twin with embedded AI:

I’m actually building a cyber digital twin for operational technology systems, so I’m actually building out a digital, virtual replica representation of an Operational Technology (OT) system. I’m having AI embedded into that digital twin. I’m actually using AI as an anomaly detector to see if there are going to be any intrusion attacks into the OT system. And at the same time, using machine learning algorithms to actually capture those signatures and create a kind of gold disc library of known and unknown attack signatures.

These two cases, while illustrative, do not represent isolated instances. Artificial intelligence and machine learning emerged as one of the most widely discussed topics across the interview data, with 26 of 27 participants addressing AI/ML capabilities in some form. This near-universal engagement reflects the degree to which AI has permeated the practitioner discourse around cyber resilience. The range of applications described was broad: participants described AI-enabled security operations centers (SOCs) in which automated triage dramatically reduced analyst response time (Participant 15), behavioral anomaly detection capable of identifying non-signature-based threats (Participant 8), automated penetration testing tools (Participant 18), and LLM-assisted code analysis for vulnerability detection (Participant 19). Participant 7 articulated a principle that surfaced across multiple interviews: “AI is only as good as the human that programs it. So, you know, I believe automation, if done correctly with buy-in and codified requirements, can absolutely provide a lot of benefits.”

However, the findings revealed a persistent deficiency in deep data expertise. Most analysts are basic inputs who lack the knowledge required to operate these tools, let alone the more profound understanding needed to address the larger, more complex problems that large organizations face. Most organizations rely on processes and repeatable playbooks rather than on understanding, which contradicts the presumed

efficiency of deploying sophisticated tools. They are underutilized, further highlighting a human-knowledge and experience gap that limits organizations' ability to become more cyber-resilient.

Theme 5: Threats, Risks, and Vulnerabilities

Participants demonstrated broad expertise and a clear understanding of the sophisticated nature of modern cyber threats. They frequently cited common attack vectors, including identity theft, exfiltration of Personally Identifiable Information (PII), ransomware, and phishing. This awareness among participants is corroborated by the foundational literature, which indicates that organizations should develop resilience strategies centered on four key abilities: planning and preparing, absorbing, recovering, and adapting to both known and emerging threats (USDHS, 2011).

The central finding highlights a consensus among participants that building cyber resilience is inseparable from a comprehensive, organizationally aligned risk management program. Participants directly stated that organizations require a strong foundation in risk management and that a comprehensive risk management program, headed by a chief risk officer, is necessary and should work with the CISO, because they need to understand the organization's risks to prioritize protecting the highest risks. This is directly supported by Linkov et al. (2013). Another direct finding supporting the need for a comprehensive risk program is that when organizations do not know which risks are critical, they cannot prioritize, link assets to critical processes, and allocate resources effectively. This finding suggests that within most participants' organizations, everything is critical and therefore nothing really is.

Theme 7: Implementation Challenges and Obstacles

The effective implementation of cyber resilience is often thwarted by tool complexity and redundancy. Organizations are buying redundant tools, which creates significant operational challenges. Participants identified that frameworks intended to facilitate implementation of cyber-resiliency or cybersecurity best practices were often confusing, depending on the organization, leading to "box checking" rather than a cohesive and tailored approach. Participant 5 captured this dynamic, noting that the issue was "because the framework is just so voluminous or it's hard to interpret it or it's hard to implement it or they just don't have the willpower to implement it." Participant 7 critiqued the lack of actionable guidance:

If it doesn't have either of those, then it's just another document that looks good on paper that someone can say, I can hold you accountable to. But again, if I can't action it in a way that my people understand what they're doing, okay.

Participants also noted that the most significant barriers to effective resilience were not technical. Participant 3 was emphatic: "The challenges are not necessarily technical. They are social. They are human. It's training, workforce, and budget." Participant 7 reinforced the workforce dimension by observing that "half my problem is now, I get more Secure Technical Implementation Guides (STIGs) than I have time or manpower to implement efficiently."

Tool redundancy compounded these workforce constraints. Participant 3 observed that organizations were "probably investing in too many redundant tools" rather than making risk-based investment decisions. Participant 11 illustrated the redundancy problem within individual products:

So, they have all of these, like add-ons and instances that the salesperson bought, but the monitoring person only uses one segment, but they're paying, you know, for the whole kit. But they have, like, six different instances that do the exact same thing.

These findings demonstrate that even when tools possess the necessary capability, if they are not selected, trained for, configured, or utilized correctly, they hinder rather than support cyber resilience.

Discussion of Findings

This section interprets the findings in light of the literature, organized by the four themes that informed the analysis of the research question.

The Philosophical Shift to Assumed Compromise

This finding contrasts with the historically dominant focus and definitions of older cybersecurity standards, which emphasized threat prevention. Prior literature by Gardner (2019) supports this, identifying that many security frameworks were initially designed to focus on prevention rather than resilience. When a security program prioritized recovery, continuity, and operational resilience, it exhibited a theoretical shift toward resilience, supported by the philosophy that cyber resilience must be integrated into existing cybersecurity frameworks. This aligns with the understanding that information security standards often focus primarily on traditional security concerns rather than integrated resilience, as discussed by Taherdoost (2022).

The Need for a Shared Resilience Lexicon

The findings showed that having a consistent, shared lexicon was pivotal in getting the community of cyber practitioners to agree upon what cyber resilience is, so that it can be resourced and implemented effectively. For cyber resilience to be considered successful, it must be measured using clearly defined criteria. Governance and the metrics that support it should shift away from purely preventive control adherence to quantifiable measures of recovery timelines.

Tools, AI/ML, and the Human-Knowledge Gap

Achieving tool and technology effectiveness is more complex than simply buying the most sophisticated options on the market and deploying them within the organization. Best practices must shift from technical purchasing toward rationalization of the tool stack and resolving the human expertise gap within the organization. No matter how complex or compelling the tool is, if the human cannot operate it, then it is ineffective. Protecting the organization requires a focus on enabling the data inherent in the tools to gather relevant insights and speed up the current process of integrating, correlating, and translating complex data into actionable, timely insights.

Risk-Based Prioritization as the Operational Foundation

Adequate protection requires risk-based prioritization. Best practices should emphasize understanding the criticality of assets to ensure resources are focused on the organization's most valuable functions. The criticality of assets and the effective management of resources should be achieved through an enterprise risk management program that incorporates cyber and information technology risks and directly addresses cyber resilience.

Implementation Realities: Frameworks, Workforce, and Tool Overload

Achieving resilience requires organizations to confront implementation challenges stemming from strategic and execution failures, not just a lack of resources. Organizations must focus on standardizing their tool stack, simplifying and tailoring frameworks to meet specific operational needs, and investing in capabilities to integrate complex data streams, rather than simply acquiring the latest tool. The theory underlying a framework's translation into practical action often contradicts its intended purpose of standardizing organizations' cyber practices and simplifying best practices; blind adherence to frameworks is ineffective and is very common among practitioners within their organizations.

Presentation of the Main Contribution

The primary contribution of this study is empirical evidence that cyber resilience is not achieved solely through tools; it requires alignment between strategic intent, organizational discipline, tactical implementation, and continuous learning and adaptation. The study presents cyber resilience as an integrated discipline that brings together tools, technology, and people to align technical capabilities with governance.

Four specific contributions follow. First, the study reinforces risk-based prioritization, grounded in the disciplined identification of critical assets, as the operational foundation on which all other cyber resilience capabilities depend. Participants made the case that when organizations cannot determine what is critical, they treat everything as critical, and therefore prioritize nothing—a condition under which neither traditional cyber tools nor AI- and ML-enabled capabilities can be effectively directed. Second, the findings reinforce the evolving view that cyber resilience is a distinct discipline from traditional business continuity and disaster recovery, with practitioners describing resilience as the ability to withstand an attack, recover quickly, and maintain essential operations during a compromise. This supports the premise in NIST SP 800-160 v2 that a breach is inevitable. Third, the findings challenge the notion that having a framework automatically makes an organization resilient. Frameworks can be a point of origin, but unless they are contextualized to the organization, they are only as useful as the paper on which they were printed. Fourth, the study extends traditional risk management thinking by showing that people and organizational culture are as critical to an organization as technology or processes are. Models of cyber risk that would best inform cyber resilience best practices should account for culture, leadership engagement, practitioner engagement, and workforce capability as key measures of risk management.

Implications for Research and Practice

The implications of this study span both theoretical contributions to the cyber resilience literature and practical guidance for organizations seeking to operationalize resilience capabilities.

Implications for Practice

Organizations should treat cyber resilience and cybersecurity as core business functions, rather than as a project implemented annually or semi-annually. Cyber resilience should be embedded within governance structures, monitored and measured through enterprise risk management, and linked to executive accountability. Organizations must take a more integrated approach across the data, cyber, legal, operational, and executive teams to ensure that cyber resilience planning delivers business or mission value. Addressing workforce limitations is a critical implication: organizations should allocate resources for ongoing training and skills development, and the skills valued and invested in should align with resilience outcomes embedded in organizational risk, business, and mission objectives. Resilience should be embedded within cyber capabilities, such as Incident Response and BC or DR plans. Metrics should be assigned to resilience capabilities, and they should be exercised and proven as much as possible. These efforts should be grounded in automation whenever possible and tracked with the most effective data analytics pipeline the organization can afford to build, staff, and maintain.

Implications for Research

Future resilience models should shift their focus from prevention to recovery through adaptive operations, prioritizing assets and exercising governance. Models of cyber risk that would best inform cyber resilience

best practices should account for culture, leadership engagement, practitioner engagement, and workforce capability as key measures of risk management. Future research should prioritize the development of a standardized lexicon for cyber resilience. The terminology problem identified in Theme 1, where cyber terms were described as “overloaded...to mean all things to all people” (Participant 21), is an operational barrier as much as a semantic one. The author and colleagues are pursuing this lexicon development effort as a separate line of inquiry. Additionally, a major focus area for cybersecurity and cyber resilience in the future is the short- and long-term impact of AI and ML on cyber resilience, including the extent to which trust is placed in autonomous systems without human oversight.

Limitations

This study has several limitations. First, the study's qualitative nature inherently limits the generalizability of the findings. The final sample was disproportionately weighted toward senior-level participants (55.56%), with only one individual categorized as entry-level (3.7%). Second, reliance on self-reported data introduces the possibility of bias due to retrospective recall. Third, the researcher's bias as a cybersecurity subject matter expert who conducted the research introduces a risk of confirmation bias during the iterative process and code matching. Finally, this study is temporal in nature and was conducted during a rapidly evolving period in cybersecurity; the findings represent a snapshot of the state of cyber resilience at the time of the study and should be interpreted accordingly.

Conclusions

The researcher contends that the concept of cyber resilience will ultimately supplant the static notion of prevention in cybersecurity, enabling organizations to focus on achieving resilience rather than relying solely on traditional approaches to preventing cyberattacks. The cyber threat environment continues to evolve, marked by increasingly sophisticated adversaries and rapidly advancing technologies that constantly shift the balance of power between offense and defense. This dynamic landscape requires organizations to maintain continuous readiness, as attackers exploit any available vector to compromise networks. To remain secure, organizations must be prepared to protect against, respond to, and recover from incidents.

The next generation of cyber practitioners must adopt the philosophy that resilience is a fundamental attribute of operational cybersecurity, grounded in the alignment of organizational strategies and governance. By integrating people, clarifying governance, prioritizing resources by risk, and continually measuring cyber resilience capabilities, a cyber-resilient mindset will be seeded in each practitioner's mind. This continuous mindset should become the standard of highly resilient cyber organizations.

Acknowledgements

The author acknowledges the use of generative artificial intelligence tools during the preparation of this manuscript, in accordance with the Issues in Information Systems AI Use Policy. Generative AI was used to support idea organization, structural drafting, language refinement, and editing of text derived from the author's original doctoral research. All substantive analysis, interpretation of findings, and conclusions are the author's own work, drawn directly from the underlying qualitative study. No participant data, interview transcripts, or other confidential research materials were processed through cloud-based or externally

hosted AI services. The author has reviewed all AI-assisted output for accuracy and attribution and accepts full responsibility for the originality, validity, and integrity of the content of this manuscript.

References

- Akcadag, E. (2012). The integration of cybersecurity into national strategy: Threats and responses. *Journal of Cyber Policy*, 1(1), 1–4.
- Bodeau, D., & Graubart, R. (2011). *Cyber resiliency engineering framework*. MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf
- Bodeau, D., Graubart, R., & Fabius-Greene, J. (2010). Improving cybersecurity and mission assurance via cyber preparedness (cyber prep) levels. In *2010 IEEE Second International Conference on Social Computing* (pp. 1147–1152). IEEE. <https://doi.org/10.1109/SocialCom.2010.170>
- Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42(8), 1643–1669. <https://doi.org/10.1111/risa.13687>
- Carias, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber resilience progression model. *Applied Sciences*, 10(21), Article 7588. <https://doi.org/10.3390/app10217588>
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, 11(10), Article 4580. <https://doi.org/10.3390/app11104580>
- Gardner, M. (2019, December 3). What's the difference between cybersecurity and cyber resilience? *Mimecast Blog*. <https://www.mimecast.com/blog/whats-the-difference-between-cybersecurity-and-cyber-resilience/>
- Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over- and under-regulation. *Risk Analysis*, 37(8), 1644–1651. <https://doi.org/10.1111/risa.12729>

- Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4), 471–476.
<https://doi.org/10.1007/s10669-013-9485-y>
- Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.
- Morgan, S. (2016). *Cybersecurity ventures predicts cybercrime damages will cost the world \$6 trillion annually by 2021*. Cybersecurity Ventures.
- Mylrea, M. (2018). *A brave new world at the cyber-energy nexus: A case study on organizational change and cybersecurity resilience* (Publication No. 10751003) [Doctoral dissertation, University of Colorado Denver]. ProQuest Dissertations & Theses Global.
- National Institute of Standards and Technology. (2023). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Rev. 1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-160v2r1>
- National Institute of Standards and Technology Computer Security Resource Center. (2024). *Glossary*. <https://csrc.nist.gov/glossary>
- O’Leary, Z. (2017). *The essential guide to doing your research project* (3rd ed.). SAGE Publications.
- Pearlson, K. (2024). When cyberattacks are inevitable, focus on cyber resilience. *MIT Sloan Management Review*. <https://sloanreview.mit.edu/article/when-cyberattacks-are-inevitable-focus-on-cyber-resilience/>
- Pool, P. (2013). War of the cyber world: The law of cyber warfare. *International Lawyer*, 47(2), 299–323.
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). *Developing cyber-resilient systems: A systems security engineering approach* (NIST SP 800-160 Vol. 2). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-160v2>
- Symantec. (2019). *Internet security threat report* (Vol. 24). Symantec Corporation.
- Symantec. (2023). *Threat landscape report*. Broadcom.
- Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards: A review and comprehensive overview. *Electronics*, 11(14), Article 2181.
<https://doi.org/10.3390/electronics11142181>

U.S. Department of Homeland Security. (2011). *Risk management fundamentals: Homeland security risk management doctrine*. U.S. Department of Homeland Security.

Watson, M. (2019). Top 4 cybersecurity frameworks. *IT Governance USA*.
<https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks>