ISSN: 2473-4901
v12 n6817

"It is Not Enough to Just Recover": Strategies, Business Alignment, and Cyber Resilience in Practice

Brian Messa
Brianmassa1987@gmail.com
Robert Morris University
Pittsburgh, PA

Abstract

Cyber resilience has emerged as a strategic necessity as organizations accept that adversaries will eventually compromise their systems. While engineering frameworks describe what resilient systems should look like, far less is known about how organizations select, resource, and sustain resilience strategies. This paper reports a subset of findings from a doctoral study (Author, 2025) that examines this question through a general qualitative study of 27 semi-structured interviews with cybersecurity practitioners across the public, private, and non-profit sectors. The findings indicate that the strategies practitioners associate with durable resilience rest on a small set of foundational controls, particularly Identity and Access Management (IAM), exercised incident response, and documented governance, but that participants described these controls as effective only when leadership builds a supportive culture and practitioners articulate the value of resilience in business terms. As one participant put it, "it is not enough to just recover. You have got to be able to be resilient." The strategies participants described as funded, staffed, and sustained were the ones they could defend in business terms. The paper contributes a practitioner-grounded model of resilience strategy sustainment, in which technical discipline, leadership-supported culture, and business alignment operate as mutually reinforcing conditions, and identifies implications for practitioners, executives, and information systems education.

Keywords: cyber resilience, cybersecurity strategy, business alignment, organizational culture, cybersecurity governance, cybersecurity workforce

"It is Not Enough to Just Recover": Strategies, Business Alignment, and Cyber Resilience in Practice

Brian Massa

1. INTRODUCTION

As cyber incidents become increasingly difficult to prevent, organizations face not only whether they can stop an attack, but also how they will operate through one. This shift is codified in NIST Special Publication 800-160 Volume 2, which defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources" (National Institute of Standards and Technology [NIST], 2023, p. 75) and rests on the premise of assumed compromise, the mindset that the adversary "will compromise or breach the system or organization" (Ross et al., 2019). The growing practitioner literature argues that prevention-centered doctrine is no longer sufficient on its own (Gardner, 2019; Pearlson, 2024).

Accepting that premise raises a practical question that engineering guidance does not answer: what strategies do cybersecurity practitioners report their organizations using to strengthen cyber resilience, and what do they describe as determining whether those strategies endure? Frameworks can specify capabilities, but strategies are executed by people, funded by executives, and sustained, or starved, by organizational culture.

This paper is based on a doctoral dissertation (Author, 2025), a general qualitative study comprising 27 semi-structured interviews with cybersecurity practitioners across the public, private, and non-profit sectors. The parent study identified nine themes addressing three research questions: (RQ1) What tools and techniques do cybersecurity practitioners recommend for building cyber-resilient organizations? (RQ2) What strategies are being employed to make organizations more cyber-resilient? (RQ3) How effective are current frameworks in guiding the implementation of cyber resilience measures? This paper examines a specific facet of that broader study: RQ2.

Theme selection follows the parent study's mapping of themes to research questions: of the nine themes identified in Author (2025), this paper examines the three associated exclusively with RQ2 (strategies and processes, human and cultural factors, and business alignment), together with two shared themes (implementation obstacles and motivation drivers) treated only as they bear on strategy execution. A companion paper (Author, in press) examines prioritization and tooling under the study's first research question, and framework effectiveness (RQ3) is reserved for future work. No participant quotation presented here appears in the companion paper.

The analysis develops a three-condition model of resilience strategy sustainment: participants repeatedly associated strategies that were funded, staffed, and maintained with the joint presence of disciplined foundational controls, a leadership-driven organizational culture, and an articulation of resilience value in business terms. In the words of the participant whose statement gives the paper its title: "It is not enough to just recover. You have got to be able to be resilient" (Participant 3). In these accounts, what carries organizations past recovery into resilience is rarely technology; it is whether trained people execute the strategy within a supportive culture and defend it in the business's own language.

2. LITERATURE REVIEW

2.1 From Prevention to Resilience

The intellectual foundation of cyber resilience lies in systems security engineering. NIST SP 800-160 Volume 2, in both its original form (Ross et al., 2019) and Revision 1 (NIST, 2023), frames resilient systems as those engineered to anticipate, withstand, recover from, and adapt to compromise. This orientation now extends to governance: the NIST Cybersecurity Framework (CSF) 2.0 introduces a Govern function that ties cybersecurity strategy to organizational mission, stakeholder expectations,

and enterprise risk management (NIST, 2024). MITRE's Cyber Resiliency Engineering Framework (CREF) established the goals-objectives-techniques structure on which much of this guidance rests (Bodeau & Graubart, 2011), and the earlier Cyber Preparedness Methodology connected preparedness levels to the sophistication of the threat an organization faces (Bodeau et al., 2010). The U.S. Department of Homeland Security (2011) describes resilience in similar terms of preparedness.

A second body of work addresses resilience as an organizational, rather than purely technical, property. Linkov et al. (2013) argue that resilience metrics must span the physical, information, cognitive, and social domains, and that resilience concepts must be integrated with risk-based management approaches. Gisladottir et al. (2017) demonstrate that regulatory regimes shape resilience outcomes and that efforts focused on rules and computers while ignoring human behavior have historically failed. Mylrea (2018) documents, in a case study at the cyber-energy nexus, that organizational change, meaning leadership, culture, and governance, is the vehicle through which resilience is actually adopted. Carías et al. (2020) propose a cyber resilience progression model that treats resilience as a maturing organizational capability rather than a one-time implementation. Most recently, Pearlson (2024) observes that prevention is structured and easy to justify, while resilience has a "softer" return on investment, which leaves resilience investments chronically disadvantaged in budget conversations.

2.2 Frameworks and Strategy in Practice

Practitioners approach these ideas through frameworks. Comparative reviews catalog an expanding landscape of NIST CSF, the ISO/IEC 27000 series, COBIT, CIS Controls, and others (Taherdoost, 2022; Watson, 2019), and industry guidance urges organizations to build pragmatic security strategies that connect protection decisions to business objectives (Scholtz, 2019).

A small but growing body of empirical work has begun to examine how cyber resilience is interpreted and led within organizations. Vasudevan et al. (2022) mapped non-technical factors of organizational cyber resilience from 25 board-level interviews. Loonam et al. (2022) interviewed C-suite executives on strategic leadership for cyber-resiliency in digital enterprises. Bagheri et al. (2023) examined management perspectives on organizational cyber resilience through case studies of two Australian universities. Closest to the present work, Dupont et al. (2023) interviewed 58 practitioners, predominantly in the financial sector, and documented the tensions practitioners navigate in making sense of cyber resilience, including contested organizational rationalities between security and business leadership.

Read together, these literatures approach cyber resilience from three directions: engineering specifications of what resilient systems should be, organizational models of how resilience capability matures, and emerging empirical accounts of how executives interpret it. Existing empirical studies have provided important sector-specific and executive-level perspectives, but less is known about how practitioners across organizational contexts describe the selection, resourcing, and sustainment of resilience strategies, and why technically sound strategies so often stall. The parent study (Author, 2025) was designed to address that gap; this paper presents the strategy-focused portion of its findings, complementing Dupont et al.'s (2023) sensemaking analysis with a maximum-variation sample and a focus on strategy execution. Sociotechnical systems theory (Bostrom & Heinen, 1977), which holds that organizational outcomes depend on joint optimization of technical and social subsystems, provides a theoretical lens for these dynamics.

3. METHODOLOGY

This paper reports on a subset of findings from a general qualitative study conducted as part of a doctoral dissertation (Author, 2025). Following institutional review board approval in June 2024, participants were recruited through the researcher's personal and professional networks — using purposeful, maximum variation, and critical case sampling (Creswell & Creswell, 2018) to counterbalance network-based recruitment — with three eligibility criteria: a minimum of five years of cybersecurity experience, classification as entry-, mid-, or senior-level, and work experience in the government, private, or non-profit sector. The final sample comprised 27 practitioners: one entry-level (3.7%), 11 mid-level (40.7%), and 15 senior-level (55.6%), with sector experience spanning government (including the Department of Defense and state and local government), the private sector, and non-profit

organizations; more than a third had worked across multiple sectors. Appendix A provides per-participant demographics. All participants provided written informed consent.

Two characteristics of this sample are relevant to the present paper's research question. First, because strategy formation and resource allocation are leadership concerns, the sample's weighting toward senior practitioners, many with direct experience advising or serving in executive functions, provides an informed vantage point on how resilience strategies are funded and sustained. Second, the deliberate variation across sectors surfaces how strategies shift with organizational mission and resource envelope, from federal agencies to higher education to commercial enterprises.

Interviews lasted 45 to 60 minutes, followed a semi-structured protocol developed by the researcher and validated through committee review and IRB approval, administered identically to every participant, and were conducted and recorded via Zoom; recordings were transcribed in the aTrain transcription application and then destroyed under the study's data-handling procedures. Analysis, grounded in a constructivist epistemology and relativist ontology, followed Creswell and Poth's (2018) qualitative data analysis spiral: an iterative process of coding, categorizing, and synthesizing. Each transcript was read twice with field-note capture; the researcher's keyword patterns were then checked against a separate software-assisted keyword frequency analysis of all 27 transcripts and field notes in NotebookLM, and the two analyses were compared before codes were consolidated in an external codebook. Coding was performed by a single researcher; the study did not employ inter-rater reliability analysis or member-checking. Each new transcript was compared against the accumulated analysis; the final interviews reinforced existing patterns without generating new categories, and by interview 27, no additional patterns were judged to have emerged. The analysis produced 11 categories that were synthesized into nine themes.

For this paper, the three RQ2-exclusive themes and their underlying categories were reread against the full transcripts; quotations were selected for evidentiary fit to RQ2 and verified verbatim against the source transcripts, including quotations beyond those presented in the dissertation. Participants are cited by number (Participant 1 through Participant 27). The parent study (Author, 2025) documents the complete protocol and analysis procedures, which are summarized in Appendix A. The interview questions are reproduced in Appendix B.

4. FINDINGS

The findings follow the resilience strategy sustainment model's three conditions: the strategies and controls organizations deploy (Theme 3), the human and cultural conditions under which those strategies are executed (Theme 6), and the business alignment that determines whether they are resourced (Theme 8), followed by two shared themes that act on strategy from outside (Themes 7 and 9).

4.1 Theme 3: Strategies, Practices, and Processes for Resilience

Participants described effective cyber resilience strategies as combinations of foundational controls tailored to the organization's threats and resources, rather than as novel technologies. The control participants emphasized most consistently, and the parent study's principal finding on effective capabilities (Author, 2025), was Identity and Access Management (IAM). Participant 20 was explicit: "I am going to double down on identity. I am going to say that emphasis and understanding of identity are key. Like, and it's been said many years ago, identity is the new perimeter. Moreover, there's a lot of truth to that one that was stated."

A second recurrent strategy was Incident Response (IR). Participants treated a rehearsed, repeatable IR capability as the mechanism that converts resilience from aspiration into practice. Participant 9 recalled, "It is got to be an incident response plan to how do you quarantine the systems you think are impacted or whatever and stop it from spreading throughout your whole enterprise. How quickly can you do that?"

Critically, participants did not treat plans as sufficient; they emphasized exercising them. Participant 3 framed exercises as both preparation and proof to leadership: "What are the procedures that are going to be followed? What are the staff trained to do? Are there simulations? Are there exercises? What are

you doing to demonstrate to your leadership … that you can respond and recover and get back operationally as soon as possible?" Participant 6 used a sports analogy to describe the payoff of rehearsal during a real crisis: "we ran this play in practice. We are now running this play in the game." The exercise, in this account, is what removes fear of the unknown from the actual incident. Adversarial validation played the same role on the technical side. Participant 15 explained, "you cannot fix or prepare for things that you do not know about. So, you know, pen testing is a great exercise."

These controls only cohere as a strategy when they are codified. Participants repeatedly grounded their strategy in uniform, documented governance. Participant 7 explained: "It gives us a process to follow, and it is a uniform process across the enterprise. One of the worst things that we can do, in my opinion, from a tactical and process level, if we are all running around doing different things, there is no way to define resiliency." Participant 18 similarly credited environments "where we had pretty well documented policies, procedures, and playbooks." Participants also described data protection practices such as end-to-end encryption (Participant 14). Through these accounts, participants characterized effective strategy less by breadth of technology than by depth of implementation: a small set of foundational capabilities, codified uniformly and rehearsed until routine.

4.2 Theme 6: Human, Organizational, and Cultural Factors

Participants were emphatic that the decisive variables in strategy execution are non-technical. The human in the loop remains both the most critical component and the most persistent vulnerability. Participant 1 stated: "the hands down most important thing is having people that do not do stupid things … There is no amount of control. There is no amount of technology or process you can use to overcome people by making mistakes and making bad decisions. And that comes from a culture, an organizational culture." Participant 4 drew the more radical conclusion: "if you want to be resilient, take the human out of the loop." This is a genuine divergence rather than a variation: where most participants proposed shaping human behavior through culture and training, Participant 4 proposed engineering human discretion out of critical paths — though full automation of such discretion is neither advisable nor realistic in most organizational contexts. Participants converged on the human as the decisive variable but diverged on the remedy of cultural investment versus automation, a tension future work should examine.

Training was consistently identified as the first strategic investment. Participant 2 argued: "you can have the perfect network in the world. You've got the most secure network in the world, but if you don't have the people that are actually trained and have … the mindset … like, Hey, cyber starts with me as well … I think the first step is making sure that the people are trained and that they know about cybersecurity and cyber awareness." Participant 1 described embedding that mindset from an employee's first day: "organizations can also have that security first mentality when they're bringing people on board. And it can be like the first, literally the first thing you can talk about in your onboarding is like, welcome to the company. Here's how we protect our company and our people and the customers that use us."

Beyond awareness, participants identified a deeper human-knowledge gap, a lack of deep data expertise distinct from headcount shortages. Participant 27 located the industry's maturity problem in "our overall understanding of cybersecurity from a data perspective. And that is from a high level, all the way down to a very granular level." Culture, in participants' accounts, is set by leadership. Where leadership engages, and resources follow. Participant 18 described the mechanism: "if it raises up to the highest level, to the cabinet, they talk about and they say, hey, the Chief Information Security Officer (CISO) said that we need to do this, to be compliant with that. And we agree. So, here's the money, go hire people and buy the thing." Effective leaders also enforce functional clarity. Participant 6 described crisis management roles: "you're here because you exist to do this, and that's your role. That's your swim lane. I expect you to kill your swim lane." Where leadership disengages, the strategy dissolves: Participant 12 described environments where teams "start spinning up whatever they want" and "cybersecurity is playing catch-up because they have no idea what's going on." These characterizations of frontline behavior rest disproportionately on senior practitioners' perspectives, given the single entry-level participant in the sample. Participants associated strategy endurance with leadership-created cultural conditions, such as trained people, clear roles, and engaged executives, under which the technical layer can operate.

4.3 Theme 8: Business Alignment and Resource Constraints

The findings under this theme explain why participants described technically similar strategies as thriving in one organization and starving in another: in their accounts, resilience efforts that are not linked to the core business mission are inadequately funded. Participant 6 stated the business-centric view bluntly, describing a logistics enterprise: "we exist to move packages from one place to another profitably." Any resilience strategy in that organization is evaluated against that sentence. In the same participant's words, "cyber resilience is just about assuring that your business is able to be resilient and it's way to make money, right?" Participant 4 illustrated the same point with a data example: "a bank's transaction information from a network guy is just data flowing. But to that bank, it's whether they're bankrupt or not, right?" Participant 17 described alignment as a maturity marker: mature organizations "adjust that strategy to actually be less, less template and more realistic on what they're going to do and what they need to do to support the business."

Resource constraints sharpen the alignment requirement, particularly for smaller organizations. Participant 19 observed that smaller organizations often cannot "invest and build something from scratch." Participant 18 offered a concrete higher-education example: "If I had an unlimited budget, I went to my boss and said, I'd like to buy these tools. Maybe at a place like MIT, they can do that, or an Ivy League, a big money school. But most of the schools that I know … we don't have the kind of budget to put into controls that are identified in that." Participant 12 cataloged what under-resourced environments look like in practice: "poor identity and access management, poor business continuity and disaster recovery, no data management, no asset management."

Participants converged on a practical answer: translate resilience into quantified business terms, most effectively by tying it to Business Continuity and Disaster Recovery (BC/DR) constructs that executives already understand. They were equally clear that resilience exceeds those constructs. Participant 3 described organizations "moving from just cybersecurity business continuity to an overall discussion about resilience in the environment. You know, it's not enough to just recover. You've got to be able to be resilient." BC/DR, in other words, is the language in which resilience value is most legible to executives, not the ceiling of the capability itself. Participant 15 advised, "the best way to get them to do something is to actually show them the return on the investment … If you can tie it to something that means something to the business from a data perspective or from a metric standpoint, then that will be very beneficial," adding the formulation, "If I'm down X hours, it costs me Y thing" — the financial impact attributable to operational downtime, known in the industry as Business Interruption (BI) Loss.

The fullest statement of this theme came from Participant 7:

> what a lot of people don't realize is that cyber resiliency is a narrative. If you can't, at a layman's term level, be a proponent for cyber resiliency for people that know nothing about cyber to get their buy-in and their support, then it doesn't matter how much framework you have, what's downward directed, they're the ones that are gonna enable your success. So, I have got to be able to spin that narrative in a way that I get buy-in, especially from leadership, to support my efforts.

Participant 26 reduced the same finding to a single line: "leadership buy-in is probably the most important thing."

In participants' accounts, business alignment is what determines whether a strategy gets resourced. It does not make a strategy technically sound, but it decides which technically sound strategies actually get funded.

4.4 Shared Themes: Obstacles and Motivation as Strategy Constraints

Two shared themes, implementation obstacles (Theme 7) and motivation drivers (Theme 9), act on RQ2 as constraints on execution. The obstacles themselves (framework complexity, tool redundancy, and staffing shortages) are examined in the Author (in press); through this paper's strategy lens, they dilute execution: Participant 11 described customers with "tool overload," having "to go log into 50 different screens" to monitor their environment, a portfolio that consumes budget and attention the strategy needs elsewhere.

ISSN: 2473-4901
v12 n6817

Motivation operates on strategy from two directions. Externally, compliance functions as the most reliable forcing function: "compliance is the main driving force behind it … at least from the commercial side of the house" (Participant 1). Internally, however, participants described a recognition imbalance that undermines the defensive work on which resilience depends. Participant 13 explained: "Defense on the other hand, you only, you only get remanded [sic] for when someone gets in rather than preventing all the other times, they did not get in." The counterweights participants offered were intangible but deliberate: giving practitioners "the why" (Participant 10) and "congratulating the team when we do a good job remediating the residual risk" (Participant 20). Framework effectiveness itself (RQ3) is reserved for future work in this program.

5. DISCUSSION

Assembled, the findings describe a resilience strategy sustainment model built on three mutually reinforcing conditions that participants associated with strategies that were funded, staffed, exercised, and maintained. The model is deliberately narrow in what it explains. It addresses strategy sustainment, meaning whether a resilience initiative survives and matures inside its organization, not measured resilience performance, which interview data cannot establish. The conditions are simultaneous rather than sequential: organizations do not complete one before beginning the next. Where maturity models such as the cyber resilience progression model (Carías et al., 2020) describe the stages a capability moves through, this model describes the organizational mechanism that resources and sustains each stage. This structure maps onto sociotechnical systems theory (Bostrom & Heinen, 1977): controls constitute the technical subsystem, culture the social subsystem, and alignment the mechanism of joint optimization. Figure 1 illustrates these relationships.

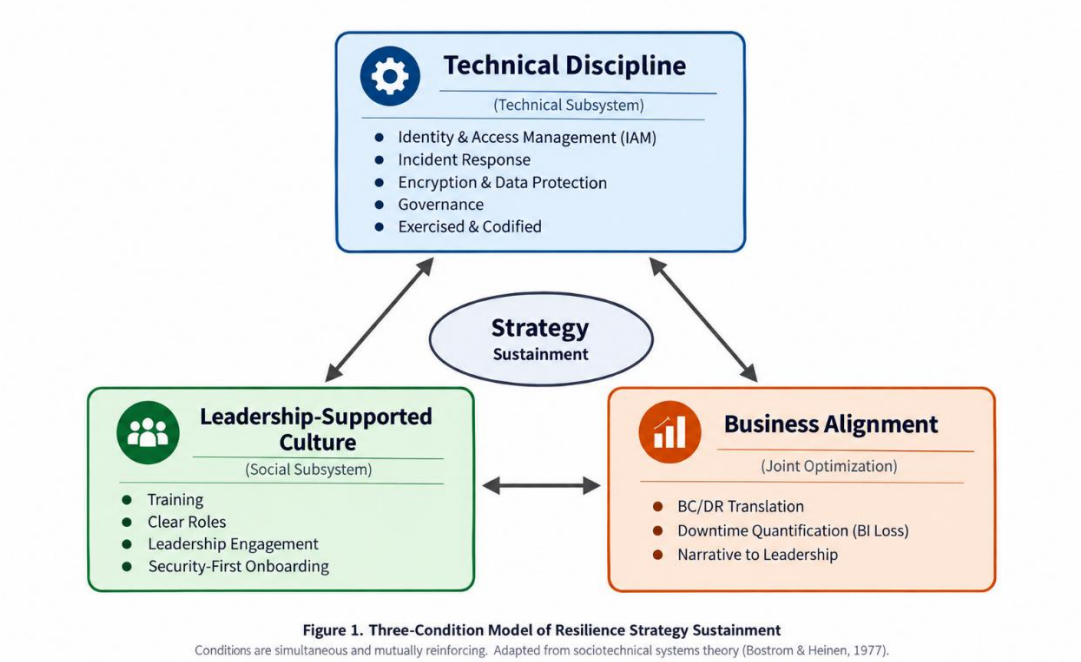

Figure 1. Three-Condition Model of Resilience Strategy Sustainment. Conditions are simultaneous and mutually reinforcing; the model describes sustainment, not measured performance.

The first condition is technical discipline: a small set of foundational controls (IAM, exercised incident response, encryption, and uniform, documented governance) implemented well rather than a large portfolio implemented thinly. This is consistent with Carías et al.'s (2020) observation that the complexity of cyber resilience demands uniformity, and with security engineering principles codified in NIST SP 800-160 (NIST, 2023; Ross et al., 2019). Participants' insistence on exercising these controls

(Participants 3, 6) echoes the literature's emphasis on measurable recovery capability rather than control existence (Linkov et al., 2013).

The second condition is human and cultural. Participants located both the greatest vulnerability and the greatest leverage in people: culture set at onboarding, sustained training, functional clarity in crisis roles, and leadership engagement that converts security requests into funded actions. This is consistent with Gisladottir et al.'s (2017) finding that resilience efforts fail when they focus on rules and computers while ignoring human behavior, and with Mylrea's (2018) account of organizational change as the vehicle for resilience adoption. The human-knowledge gap identified here, meaning depth of data expertise as distinct from headcount, adds practitioner detail beyond the familiar skills-shortage framing.

The third condition is business alignment, which participants described as determining whether the first two are resourced. Participants' testimony was consistent: resilience strategies compete for funding in a language their sponsors may not speak, and practitioners have to do the translating. Pearlson (2024) observes that resilience carries a softer return on investment than prevention; practitioners in this study described the practical remedy: anchoring resilience value in BC/DR terms and downtime costs that executives already quantify. The "narrative" formulation (Participant 7) captures the finding precisely: alignment is not a document but an ongoing act of persuasion, renewed at every budget cycle. This finding also offers cross-sector support for the contested organizational rationalities Dupont et al. (2023) observed among financial-sector practitioners: security practitioners and business leaders reason from different premises, and the practitioner has to translate between them.

It is worth considering an alternative: perhaps compliance, not alignment, is what actually funds resilience. Participants described external mandates as the most reliable forcing function for security spending (Section 4.4), and such mandates can compel investment where alignment alone would not. But the same participants described what compliance-driven funding buys: controls implemented to the letter of an audit rather than to the organization's actual risk (Author, 2025). Compliance explains why a control exists; alignment explains whether the capability around it is staffed, exercised, and sustained. The two mechanisms are complements, not substitutes, and only the second was associated, in participants' accounts, with what they recognized as resilience. The weight of each condition also varies with context: participants from smaller organizations described misaligned strategies failing faster, while larger ones carried misalignment longer at the cost of tool sprawl.

The model builds directly on the companion paper's foundation. The author (in press) argues that risk-based prioritization is the operational foundation of resilience, and that when organizations treat everything as critical, nothing is. The present findings describe what comes after prioritization: the prioritized strategy must still be executed by trained people inside a supportive culture and defended in business terms. Prioritization tells the organization what to protect; the conditions described here shape whether, in practitioners' experience, that protection is sustained.

6. IMPLICATIONS AND RECOMMENDATIONS

For practitioners, the findings translate into actionable recommendations drawn from the parent study (Author, 2025) and sharpened by this paper's analysis. First, implement a robust foundation of security controls focused on IAM and incident response before pursuing more sophisticated capabilities. Second, conduct tabletop and live cyber resilience exercises for critical systems, and operate a lessons-learned program with owners, completion plans, and metrics tracked by leadership, since participants treated the exercise, not the plan, as the unit of resilience. Third, invest deliberately in people: recruit, train, and retain skilled professionals; embed a security-first mentality from onboarding; and cultivate the deeper data expertise that the human-knowledge gap demands. Fourth, ensure cyber resilience strategies align with organizational strategies and priorities, and articulate their value in measurable terms executive leadership already understands, since participants emphasized downtime cost and BC/DR impact as the clearest translations. Finally, treat alignment as a continuing narrative rather than a one-time justification: in participants' accounts, sustained funding followed from the ability to consistently explain resilience to non-technical decision-makers.

For executive leaders, the findings assign specific responsibilities that cannot be delegated to the security function: setting up the culture, enforcing functional swimlanes, and serving as the conversion point where security requests become funded actions. The recognition imbalance participants described

rests with leadership, because organizations that notice defense only when they fail should expect to lose the defenders they need for resilience.

For information systems and cybersecurity educators, the findings translate into teachable, assessable practices. The decisive skills in participants' accounts of sustained strategy were not exclusively technical: translating technical risk into business language, quantifying downtime, and constructing an executive case shaped whether technically sound strategies survived. Programs can develop those competencies directly through executive-briefing assignments in which students present a technical risk to a non-technical audience; downtime-cost and business-impact calculation exercises of the form participants used ("If I am down X hours, it costs me Y thing"); cross-functional tabletop exercises that assign students business as well as security roles; and budget-constrained cases requiring students to prioritize controls against a stated organizational mission. Each activity maps to a competency that participants identified as decisive in practice.

7. LIMITATIONS

The limitations of the parent study apply to this paper (Author, 2025). Consistent with the study's constructivist stance, the findings claim transferability rather than statistical generalizability: the account of participants' contexts is intended to let readers judge the fit of these findings to their own organizations, not to estimate population parameters. Network-based recruitment introduced self-selection bias, and interview accounts are subject to retrospective recall and professional-image bias — practitioners describing their own field may favor strategic and leadership explanations. Critically, the study collected no independent organizational performance data: it can describe the conditions participants associated with strategy sustainment, but it cannot establish causal effects or verify resilience outcomes. The sample was disproportionately senior (55.6% senior-level, one entry-level participant), which serves the strategy focus but narrows the ground-level perspective, and no participant worked exclusively in the non-profit sector. Coding by one researcher with a cybersecurity background created a confirmation-bias risk mitigated — though not eliminated — by the iterative analysis and cross-checks in Section 3; the study used neither second-coder analysis nor participant validation. Finally, the study captures a snapshot in time; evolving regulation, threat conditions, and governance structures may alter the conditions participants described.

8. CONCLUSIONS

This study's contribution is threefold. Empirically, it supplies cross-sector practitioner evidence on how cyber resilience strategies are selected, funded, and sustained, a vantage point underrepresented in engineering guidance and in executive-level or single-sector studies. Conceptually, it develops a three-condition model of resilience strategy sustainment in which technical discipline, leadership-supported culture, and business alignment operate as mutually reinforcing conditions; the model's scope is deliberately bounded to strategy viability and sustainment, its conditions were derived interpretively rather than tested, and its transferability varies with organizational size, sector, and regulatory context. Practically, it identifies business translation, downtime quantification, and cross-functional exercise design as core professional competencies, with direct application to information systems curricula. Future research should test whether this configuration of controls, culture, and alignment predicts measurable continuity, adaptation, and recovery outcomes across sectors, and should examine the automation-versus-culture divergence this study identified. Cyber resilience strategy, these findings suggest, is not only an engineering problem but an organizational alignment problem, and treating it as such changes what both organizations and educators should build first.

9. ACKNOWLEDGEMENTS

Generative artificial intelligence tools, specifically NotebookLM (Google) for keyword frequency analysis during coding (detailed in Section 3) and Grammarly (Grammarly, Inc.) assisted with literature organization, editing, and formatting. All analysis and conclusions are the author's, and all participant quotations were verified verbatim against the original interview transcripts.

10. REFERENCES

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience: Management perspectives. *Australasian Journal of Information Systems, 27*. https://doi.org/10.3127/ajis.v27i0.4183

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

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. MIS Quarterly, 1(3), 17–32. https://doi.org/10.2307/248710

Carías, 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.

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security, 132*, Article 103372. https://doi.org/10.1016/j.cose.2023.103372

Gardner, M. (2019, December 3). *What's the difference between cybersecurity and cyber resilience?* Mimecast. 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

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2022). Cyber-resiliency for digital enterprises: A strategic leadership perspective. *IEEE Transactions on Engineering Management, 69*(6), 3757–3770. https://doi.org/10.1109/TEM.2020.2996175

Author. (2025). [Reference withheld for blind review.]

Author. (in press). [Reference withheld for blind review.]

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. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

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/

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

Scholtz, T. (2019). *Develop a pragmatic vision and strategy for digital business security* [Gartner research report]. Gartner Inc. https://www.gartner.com

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). *National preparedness system*. Federal Emergency Management Agency. https://www.fema.gov/pdf/prepared/nps_description.pdf

Vasudevan, S., Piazza, A., & Carr, M. (2022). Qualitative factors in organizational cyber resilience. In *2022 International Conference on Cyber Resilience (ICCR)*. IEEE. https://ieeexplore.ieee.org/document/9995762

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

APPENDIX A

Participant Demographics and Methodological Detail

ID	Sector(s)	Work Level	Education	Certification Type
P1	Gov & Private	Mid	Bachelor's	Cybersecurity
P2	Government	Senior	Doctorate	Cybersecurity
P3	Private	Senior	Bachelor's	Cybersecurity
P4	Gov/Non-Profit/Private	Senior	Doctorate	Cybersecurity
P5	Gov & Private	Mid	Bachelor's	Cybersecurity
P6	Gov & Private	Mid	Master's	Specialized Cyber
P7	Government	Senior	Master's	Cybersecurity
P8	Non-Profit & Private	Senior	Doctorate	None
P9	Government	Entry	Master's	Cybersecurity
P10	Government	Senior	Doctorate	Cybersecurity
P11	Gov & Private	Mid	Master's	Mixed
P12	Private	Mid	Master's	Cybersecurity
P13	Gov & Private	Mid	Master's	Specialized Cyber
P14	Private	Senior	Master's	IT/Cloud
P15	Private	Senior	Bachelor's	Cybersecurity
P16	Government	Mid	Master's	Cybersecurity
P17	Gov & Private	Senior	Master's	Mixed
P18	Private	Senior	Master's	Specialized Cyber
P19	Private	Senior	Doctorate	None
P20	Gov & Private	Mid	Bachelor's	Cybersecurity
P21	Gov & Non-Profit	Senior	Doctorate	Cybersecurity
P22	Private	Mid	Bachelor's	IT/Cloud
P23	Private	Mid	Bachelor's	Mixed
P24	Private	Mid	Master's	Cybersecurity
P25	Government	Senior	Master's	None
P26	Gov & Non-Profit	Senior	Doctorate	Cybersecurity
P27	Gov & Private	Senior	Master's	IT/Cloud

Table A1. Participant demographics: sector experience, work level, highest education, and primary certification category.

Work level reflects total professional experience: Entry = 5–10 years, Mid = 10–15 years, Senior = 15+ years. Sector categories reflect the organizational environments in which participants have worked across their careers; combined labels indicate multi-sector experience.

Protocol and data handling. A semi-structured interview protocol was administered identically to every participant, with no deviations in the question set. Interviews were conducted and recorded via Zoom, transcribed in the aTrain transcription application, and the recordings were destroyed once transcription was verified, in accordance with the study's data-handling procedures. The study received institutional review board approval in June 2024; all participants provided written informed consent, participated voluntarily, could withdraw at any time, and were assigned pseudonyms (Participant 1 through Participant 27) with organizational identities withheld.

Analysis procedure. Each transcript was read twice with repeated-keyword capture in field notes. The researcher's keyword patterns were compared against a separate software-assisted scan of the transcripts (NotebookLM); the two analyses were reconciled before code identification. Verified codes were consolidated in an external codebook and grouped into 11 categories, which were synthesized into nine themes following Creswell and Poth's (2018) data analysis spiral. Each new transcript was compared against the accumulated analysis; by the 27th interview, no additional patterns emerged. For the present paper, the three RQ2-exclusive themes and their underlying categories were reread against

the full transcripts, and all quotations, including those not presented in the parent study, were verified verbatim against the source transcripts.

APPENDIX B

Interview Protocol — Research Question Mapping

Questions QA–QB are background/suitability questions. Questions Q1–Q17 are substantive interview questions; research question mappings follow the parent study (Author, 2025, Table 4).

Question	Text	RQ Mapping
QA	Briefly describe your role as it relates to cyber or IT operations at your organization.	Background
QB	What made you choose your current role at your organization?	Background
Q1	How have organizations you have belonged to assessed their cyber risk?	RQ1, RQ2, RQ3
Q2	Have you ever had to deal with a security incident before? If so, explain.	RQ1, RQ2, RQ3
Q3	Are you familiar with the term cyber-resiliency? If so, what does it mean to you in your own words?	RQ1, RQ2, RQ3
Q4	Do any of the organizations you have belonged to architected or defined a cyber-resiliency strategy or cyber strategy?	RQ1, RQ2
Q5	Were there any rewards or incentives for effectively implementing the organization's cyber-resiliency strategy or cyber strategy?	RQ2
Q6	What tools or techniques do you or did you use the most to protect your organization?	RQ1, RQ2, RQ3
Q7	Did you think these tools helped or hindered your organization's cyber resilience as we have defined it in this interview?	RQ1, RQ2, RQ3
Q8	Are you familiar with current cyber frameworks such as NIST CSF?	RQ1, RQ2, RQ3
Q9	Has any organization you belonged to ever	RQ3

ISSN: 2473-4901
v12 n6817

	implemented one of those frameworks? If so, which one?	
Q10	Did you think the frameworks were useful to help make your organization or past organizations more resilient?	RQ1, RQ2, RQ3
Q11	Are you familiar with SP 800-160 Vol. 2 Rev 1? Are you developing Cyber Resilient Systems?	RQ1, RQ3
Q12	If you are not familiar with the resiliency framework from before, what do you think is in the framework?	RQ1, RQ2, RQ3
Q13	Do you think frameworks are useful in cybersecurity?	RQ1, RQ3
Q13a	If you answered no, what should be used in their place to make cyber organizations more resilient?	RQ1, RQ3
Q14	What is the most important thing an organization can do to be cyber resilient?	RQ1, RQ2, RQ3
Q15	What are the significant risks from cyber threats that organizations like yours need to protect against?	RQ1, RQ2, RQ3
Q16	Do you believe AI and autonomous systems would hinder or help organizations with cyber-resiliency concerns?	RQ1, RQ2, RQ3
Q17	Is there anything else you would like to share, or was there anything you would like to have been asked but were not?	RQ1, RQ2, RQ3