Columbia SIPA

Advisors: Evan Douglas Wolff & Sydney Allyson Jones

We would like to thank McKinsey for their support on this effort

May 2025

CAPSTONE REIMAGINING CYBER RESILIENCE

A Sectoral Deep Dive Into Defense, Finance, and Healthcare

Prepared by

Aashika Mehta

Abrar Ahmed

Angela To

Mika Lobell

Noa Cohen

Samuel Dab

Table of Contents

Executive Summary

As cyberattacks grow in quantity, sophistication, and impact, critical infrastructure sectors such as defense, finance, and healthcare face unique but converging challenges in maintaining operational continuity amid adversarial threats. This report explores how these sectors define, measure, and implement cyber resilience, not just to protect systems, but to ensure mission-critical functions persist through disruption.

Drawing from cross-sector and sector specific interviews, industry frameworks, and recent case studies, the report identifies common barriers, sector-specific gaps, and maturity differences across domains. While the defense sector balances inherent operational resilience with regulatory complexity and emerging tech risk, finance benefits from regulatory pressure and systemic awareness. By contrast, healthcare remains acutely vulnerable due to having fragmented oversight and thin margins.

Introduction

“Cyber resilience is misunderstood as preventing failure. It should be making failure graceful.” - Trey Herr

Why cyber resilience now?

Based on recent interviews with cybersecurity experts, this report examines how defense, financial, and healthcare organizations maintain operational continuity amid cyber threats and the complexities that challenge these efforts. Interviews with experts identify common gaps, including over-reliance on third parties, underinvestment in recovery capabilities, and regulatory inconsistencies. Shared concepts of cyber resilience include maintaining mission-critical operations and adapting to threats. However, the sectors have differing degrees of maturity: defense demonstrates operational resilience in core areas but with fragmentation, finance is generally more mature due to regulatory drivers, and healthcare faces challenges due to high digital dependency and resource constraints. Emerging technologies like AI, quantum computing, and cloud services present both opportunities and challenges for enhancing cyber resilience.

The need for robust cyber resilience has never been greater due to the escalating frequency and impact of cyber threats targeting critical infrastructure and essential services. Recent high-profile incidents, such as the attack on Change Healthcare, which caused significant operational disruptions in the healthcare sector, and the Colonial Pipeline ransomware attack, which impacted fuel supply, highlight the potential for cyber incidents to have far-reaching physical consequences beyond data breaches. These events highlight the limitations of purely preventative cybersecurity and necessitate a focus on the ability to withstand, recover from, and adapt to cyberattacks to ensure operational continuity.

Defining cyber resilience vs. cybersecurity

Cybersecurity is broadly understood as focusing on preventing, detecting, and responding to cyber threats to protect sensitive data and systems, often driven by regulatory mandates. It involves implementing security controls such as access controls, encryption firewalls, and network segmentation.

Cyber resilience, in contrast, is concerned with ensuring that organizations can continue to operate effectively, limit harm, and recover swiftly in the aftermath of a cyber incident. It emphasizes the ability to withstand threats and maintain essential functions, even under degraded conditions, and to learn and adapt from attacks to improve future responses and be stronger. Several experts view cybersecurity as the technical underpinning necessary for cyber resilience. Without security and system integrity, cyber resilience is not possible[1].

The rise of cyber threats

- The Change Healthcare cyberattack in February 2024 was unprecedented in magnitude, affecting the personal data of 190 million people - over half of the U.S. - and costing $3.09 billion causing widespread disruption in the healthcare sector, disrupting payment processing and the ability of healthcare providers to function normally for an extended period.[2] This event demonstrated the high digital dependency and low tolerance for disruption in healthcare.
- The Colonial Pipeline ransomware attack in 2021 resulted in the shutdown of a major fuel pipeline, causing significant economic and logistical challenges across the United States. This illustrates how cyberattacks can impact critical national infrastructure.
- The Israeli pager attack serves as an example of a complicated operation with devastating consequences, suggesting that commercial entities may not be adequately considering such sophisticated attacks.
- The increasing prevalence of ransomware across all sectors, defense, finance, and healthcare, demonstrates a persistent and financially motivated threat.

[1] National Institute of Standards and Technology (NIST). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, SP 800-160 Vol. 2 Rev. 1, December 2021
[2] "UnitedHealth Estimates Change Healthcare Hack Impacted About 190 Million People." *The Wall Street Journal*, 22 Apr. 2024.

Research methodology

The ***primary objective*** was to assess how sectors and organizations define and operationalize cyber resilience, evaluate the current state of best practices, and anticipate emerging threats and future solutions across sectors.

Interviews were conducted with leading cybersecurity experts from various sectors, including Alan Barry, Adam Shostack, Beau Woods, Beth Cartier, Brad Maiorino, Cameron Dicker, Charles Carmakal, Charles Gazoni, Chase Carpenter, Chris Ramey, Dean Perrine, Greg Rattray, Jason Healey, Michael Franklin, Neal Pollard, Jason Fieger, Robert Kaiser, Rob Knake, Sean Atkins, and Viet Tran. These interviews provided insights into the practical challenges, definitions, and strategies related to cyber resilience in their respective domains. These interviews aimed to validate findings from desk research, capture real-world practices and operational definitions of resilience, and understand sectoral challenges, drivers, and future trends.

Desk research took place where a comprehensive literature review was conducted to understand current definitions, frameworks (such as NIST CSF, CMMC, and ISO risk management frameworks), best practices, and sector specific risks, threats, vulnerabilities, and recovery strategies.

Cross-sectoral and sector-based deep dives and analysis of the information gathered from the interviews and literature to identify common themes, cross-sectoral comparisons, differences, and emerging challenges in achieving cyber resilience across the defense, healthcare, and financial sectors.

Forward-looking analysis where the team identified existing gaps and emerging threats to proposed potential recommendations and solutions to strengthen resilience in a rapidly evolving cyber landscape.

Cross-Sector Comparison

Common gaps and risks

Over-reliance on third parties and lack of transparency: All sectors express significant concern about the risks posed by third-party vendors and the difficulty in ensuring their cyber resilience. The opaqueness of fourth and fifth-party dependencies exacerbates this issue. Even if an organization has strong internal security, vulnerabilities in its supply chain can be exploited.

Underinvestment in recovery and continuity vs. prevention: There is a tendency across organizations to focus more heavily on preventative measures rather than investing sufficiently in response and recovery capabilities. Disaster recovery plans, often designed for physical events, are frequently insufficient for cyber incidents.

Regulatory inconsistencies and lack of clear accountability: In the defense sector, some argue that regulations like Cybersecurity Maturity Model Certification (CMMC) are overly burdensome and may not effectively enhance resilience. With healthcare there are many different sub-industries that make it difficult to regulate. For example, with medical device manufacturers, there are many different sets of incentives, capabilities, and roles to consider than with other healthcare providers such as electronic health records manufacturers, payments and billing, and insurance. “Electronic health records providers are excluded from regulation from some of the FDA's medical device regulations, even though they might fit that. There’s been a deliberate choice to not have them as a regulated entity.”[3] In general, there is a lack of a comprehensive system for assessing and addressing cyber threats at a sector-wide level. Determining accountability for cyber resilience, especially concerning cloud service providers, remains a challenge.

[3] “Cyber Regulation and Harmonization: Panel 5 on Regulating Healthcare Cybersecurity.” *Youtube*, uploaded by Columbia SIPA, 27 Nov. 2024.

Shared concepts of cyber resilience

***Differentiation from cybersecurity, reactive vs. preventative*:** Experts consistently differentiate cyber resilience from cybersecurity by emphasizing its focus on reacting to and recovering from incidents rather than solely preventing them. Resilience involves a mindset that anticipates breaches, "not a question of if but of when," and prepares for effective response and recovery.

***Continuity of mission-critical operations despite risks and threats*:** The core concept of cyber resilience across all sectors is the ability to maintain essential business or mission functions even during and after a cyberattack. This includes the capacity to operate under degraded conditions.

***Emphasis on recovery, adaptability, and minimum viable operations*:** Cyber resilience involves having capabilities and plans for rapid recovery, the ability to adapt operations and systems in response to attacks, and identifying the "minimum viable" functions that must be maintained to ensure essential services.

Differing degrees of maturity

Sector	Maturity Level	Tolerance to Disruption	Drivers of Resilience Maturity
Finance	High	High	Regulatory pressure (Fed, DORA), market stability
Healthcare	Low	Very Low	Thin margins, fragmented oversight, patient safety risks
Defense	High*	Medium	Inherent redundancy, wartime preparedness culture

Finance leads in articulating impact tolerance and executing detailed recovery plans. Healthcare, while mission-critical, lacks both centralized regulation and resources to define its tolerance. Defense straddles the line; its systems are hardened, but digital interdependencies are not always well-understood.

Emerging technology tensions

AI is powerful for defense and detection but also is a new attack surface - Artificial intelligence presents a double-edged sword for cyber resilience. It offers powerful tools for threat detection, automation, and improving defenses. It can try to sort through all the noise within milliseconds with a better hit rate than analysts, and can map out attacks in 10 seconds that would take an analyst half a day at least.[4] However, AI also creates new attack surfaces, such as model manipulation and hallucinations which can be used by malicious actors to lower the bar for attacks, and introduces risks related to the security of AI systems themselves. The rapid evolution of AI is outpacing the ability to fully understand and manage its risks. However, AI needs to be used to make your system better and smarter or organizations will be left behind

Quantum is a looming massive challenge and few are prepared: Quantum computing is a looming massive threat with the potential to break current encryption methods, posing a significant challenge to data security and resilience. While the timeframe for widespread quantum attacks is uncertain, the need for "quantum-safe" encryption and preparedness is becoming increasingly important, although few organizations are currently prepared.

Cloud is accepted but still a point of failure if not properly managed: Cloud services have been around for a while and offer potential benefits for cyber resilience, such as scalable backups, faster recovery, and distributed services. However, reliance on the cloud also introduces new risks, including third-party dependencies, data breaches, and the potential for widespread outages if cloud providers are compromised. The cloud is now deeply baked into risk management and the supply chain but proper management and security of cloud environments are still crucial for realizing their resilience benefits.

[4] Cybersecurity healthcare expert.

Sectoral Deep Dives

Defense Sector

"Built for continuity, struggling with complexity"

Industry Insights

Mission-critical operations tolerate some digital degradation

Defense operations are designed to continue even under a cyber attack, tolerating a degree of digital degradation. As one expert noted, true cyber resilience means an organization can handle problems "without grinding to a halt," effectively degrading gracefully under duress. In practice, this means critical military and industrial functions have analog or manual fallback options. For example, one defense expert observed that certain logistics tasks in the DIB can revert to "paper and pen" and manual controls to keep vital supply lines moving, albeit with difficulty. Not every system has an offline backup (modern weapons design is almost entirely digital), but minimum viable operations are defined such that if networks are impaired, core missions (like munitions production or force mobilization) can still carry on at reduced capacity. This acceptance of partial digital loss is built into continuity planning to ensure no single cyber incident can completely paralyze defense capabilities. The focus is on warfighting through cyber attacks, maintaining command, control, and critical processes even when some IT systems fail.

Resiliency is built into planning, but sectoral coordination is weak

Defense organizations extensively plan and prepare for cyber incidents, embedding resiliency into their operations. One cyber leader described how their team conducts regular tabletop simulations of worst-case scenarios, such as a simulated cyber attack coinciding with a geopolitical crisis, to test how well they could "survive and recover" under concerted attack. Such exercises help identify gaps and ensure continuity plans are in place. However, while individual companies (particularly major defense primes) invest heavily in resilience planning, coordination at the sector level remains a concern. One expert criticized the lack of a collective defense sector strategy for cyber threats, noting that it's "not a company-by-company question," the sector as a whole lacks unified programs for threat assessment and response. Another expert echoed that truly staying ahead of advanced threats (like zero-day exploits) requires much tighter collaboration between government and companies through intelligence sharing. Information sharing and joint planning do occur, for example, some defense CISO teams maintain informal chat channels to update each other on threats, but these efforts are ad hoc. Overall, cyber resiliency is built into defense planning at the organizational level, yet sector-wide coordination and shared readiness remain relatively weak, creating potential gaps in a large-scale cyber crisis.

Strong practices: zero trust, live testing, prioritization matrices

Interviews highlighted several best practices that bolster cyber resilience in defense. First is the adoption of zero trust architectures, a "never trust, always verify" approach to network access. Government mandates and initiatives have recently pushed zero trust, yielding a "significant impact" on improving defense contractors' security postures. Companies that embrace zero trust and similar modern frameworks tend to be more advanced in confronting threats, moving away from legacy perimeter defenses to continuous validation of users and devices.

Another strong practice is the "crown jewel" and stress testing of cyber defenses. Rather than relying on paper plans alone, leading organizations conduct realistic drills and "live tests" of their incident response plans. One cybersecurity leader noted that everyone can draft a plan, "but then it fails in real time" if not exercised; during a major ransomware scenario, "4,000 things happen simultaneously," and organizations quickly discover whether they have the capacity and clarity to respond. These live exercises

force teams to identify choke points and practice keeping the business running under pressure, which greatly enhances preparedness.

Crucially, such testing drives the use of prioritization matrices (or similar frameworks) to decide what to save first in a crisis. Defense firms are learning to pre-determine a "set of priorities" for systems and missions. This involves doing business impact analyses to map out the most critical services and assets, then planning how to keep those online at all costs. Having a full inventory of priorities ensures that when a cyber incident strikes, leaders know which applications or facilities must be restored first and which can tolerate downtime. In short, zero trust limits damage, crown jewel exercises reveal real-world failure points, and rigorous prioritization of assets guides effective response. These practices, already adopted by top-tier defense contractors, set a benchmark for resilience across the DIB.

Despite progress, the defense sector faces persistent cyber resilience risks that stem from the complexity of its operations and technology. Key risk areas include:

Command & Control (C2) Systems have vulnerabilities

Sophisticated adversaries may target the military's command-and-control networks and data integrity. Even if most IT can degrade gracefully, a breach in C2 systems could disrupt decision-making or weapon deployment. As one expert emphasized, the integrity of C2 communications "really matters," falsified or poisoned information in these channels can be more damaging than outright denial. Ensuring the authenticity and availability of orders and intelligence is an ongoing challenge, especially as cyber attacks blur the line between peacetime and wartime operations.

Supply chain is fragile

The defense supply chain relies on tens of thousands of smaller suppliers, many of which have immature cybersecurity capabilities. One interviewee noted that a large portion of the DIB consists of small-to-midsize companies, some without even a full-time IT department, resulting in a "low level" of cyber readiness in parts of the supply chain. This creates a weak link: an advanced adversary can target a less secure subcontractor to disrupt manufacturing of critical components or steal sensitive data. Additionally, recent geopolitical events revealed how little visibility prime contractors sometimes have into their extended supply chains. Cyber attacks on a key supplier could halt production

of important equipment, illustrating the need to bolster resilience not just within prime defense firms but across all tiers of suppliers.

Legacy platforms and "old-school" processes

Much of the defense sector still runs on legacy IT and operational technology that was not designed with modern cyber threats in mind. Even highly resourced defense primes often use manual security methods; their resilience can be "highly advanced but… very old school" with heavy reliance on human detection of issues. Legacy mission systems (from aging industrial control systems in factories to older software in weapons platforms) are difficult to patch or retrofit with strong cyber controls, creating enduring vulnerabilities. These outdated systems and processes add complexity, as integrating new defenses or technologies (like cloud services or AI tools) with legacy infrastructure is often slow and fraught with compatibility issues. The net effect is a slower response to threats and an inability to leverage cutting-edge resilience techniques uniformly across all systems. Modernizing or isolating these legacy platforms remains a significant challenge for the sector.

Key Recommendations

To address these challenges and enhance cyber resilience in the defense sector, we propose the following recommendations:

1. ***Mandate Resilience Testing Across the DIB*:** The DoD should require regular cyber wargames and exercises for all major defense contractors and their key suppliers. This will ensure that plans are not just paperwork but are tested in simulated high-pressure scenarios.

2. ***Fund Cross-Sector Systemic Risk Research Initiatives*:** Government and industry should co-fund research into systemic cyber risks. One expert noted the lack of institutions that regularly study threats specific to defense. A research consortium could help model cascading risks and propose metrics and strategies.

3. ***Integrate AI Safely for Defense (Defensive and Offensive Applications)*:** The sector should expand its use of AI in cyber defense, with robust oversight. While AI can enhance speed and accuracy, it must be tested for safety and guarded

against adversarial use. Human oversight must remain central to all AI-enabled cyber operations.

4. ***Build Shared Threat Modeling Platforms with Interoperable Standards*:** The sector would benefit from a common platform to share anonymized threat models and scenarios. One interviewee stressed that threat modeling is "really important for resiliency," yet it is still siloed. A shared portal could enable better, faster collaboration across the DIB.

5. ***Bolster Supply Chain and Legacy System Resilience*:** The DoD should expand support for small suppliers' cybersecurity and invest in modernizing or isolating legacy platforms. Cloud migration, segmentation, and zero trust controls should be prioritized to mitigate risks stemming from outdated systems and under-resourced partners.

Sectoral Deep Dives

Financial Services

"Interconnected, targeted, and regulated"

Industry Insights

Third-party and interconnected suppliers are increasing systemic risks

The financial services industry operates as a highly interconnected and technology-reliant ecosystem. As digital integration deepens across institutions, so too does the sector's exposure to sophisticated and disruptive cyber threats. In recent years, the frequency, scale, and systemic impact of cyber incidents have accelerated, often originating not from primary institutions but from smaller, highly embedded third-party providers. Recent high-profile cases such as the Ion, Equilend, and ICBC Financial Services incidents have highlighted how operational disruptions at niche service providers can propagate across markets, impairing core financial functions and testing the sector's resilience at scale.

This comes as the sector has progressively realized and acknowledged the increased dependency on third-party service providers. While outsourcing has brought efficiency and scale, it has also introduced complex dependencies that are difficult to map and even harder to govern. Visibility into fourth- and fifth-party suppliers remains limited, and institutions are struggling to assess their exposure to shared infrastructure and concentration risk. Industry experts from leading financial institutions testified[5] on the difficulty of running tabletop exercises with their third-party vendors, even though these

[5] Robert Kaiser and Jason Fiegel interviews.

have been proven to yield significant improvements in communication and resilience planning.

Communication lapses and a lack of common lexicon

One of the recurring problems for resilience has been the challenge of effective communications in times of crisis, both internally across an institution's different departments (usually the business side and the technical side), and externally with the growing number of vendor firms that are relying on. Business and technology teams often lack a shared vocabulary, and roles are frequently unclear during high-pressure scenarios. “If your tabletop didn’t surface a communication issue, you didn’t do it right,” one senior executive noted.

Widening gap: large institutions and the small players

Interviews also revealed a widening gap in resilience maturity across the sector. Large institutions with greater in-house capabilities are building integrated cyber-resilience programs, negotiating stronger terms with vendors, and having the capabilities to internally develop and manage emerging technologies such as artificial intelligence. In contrast, smaller financial institutions are increasingly reliant on third-party solutions without the leverage to demand meaningful resilience guarantees. As Robert Kaiser of BNP Paribas remarked, “The bigger you are, the more answers you’re going to get from your vendors. The smaller you are, the more you have to settle for ‘good enough.” The result is a growing divide in resilience readiness, with systemic implications.

Resiliency is increasingly under regulatory scrutiny

Finally, as their dependencies and outsourcing to third-party vendors have grown, financial institutions are facing increased regulatory pressures to manage the risks arising from their ICT third-party vendors. “You can outsource business processes, but you cannot outsource the risk,” said Robert Kaiser (BNP Paribas). New regulations, most notably the EU’s Digital Operational Resilience Act (DORA), are directly targeting the critical dependencies financial institutions increasingly rely on. Notably, DORA introduces the designation of “Critical ICT Third-Party Service Providers”, enabling direct oversight of the technology firms with substantial presence in the sector. This

might introduce an opportunity for financial institutions to demand more information and transparency over major vendors that will be designated under that label.

Together, these insights point to a financial system under pressure to adapt. Institutions are navigating more complex threat vectors, deeper dependencies, and rising regulatory expectations. In this context, resilience is no longer a static capability, it is a dynamic, enterprise-wide discipline that must be embedded across operations, technology, and governance.

Key Recommendations

Minimum Viable Bank (MVB) - a new standard for resilience planning

“A Minimum Viable Bank (MVB) is the smallest set of business functions, systems, and services that a financial institution must keep operational during a major cyber incident to uphold systemic stability, meet critical regulatory obligations, and maintain trust with key business partners and customers while operating in a degraded state”.

The MVB concept pushes firms to move beyond traditional recovery metrics and prioritize continuity of core functions under sustained disruption, rather than assuming rapid full restoration. In our interviews, several leaders emphasized that resilience decisions often falter without clear internal alignment on what truly constitutes a firm’s critical activities.

Applying the MVB lens requires institutions to take four key steps:

1. Define Minimum Viable Bank core services based on impact tolerances, revenue contribution, regulatory exposure, and systemic importance.

2. Tier all business functions by time-sensitivity and systemic impact, recognizing that criticality shifts over time.

3. Map the upstream and downstream dependencies that enable these core functions, including third- and fourth-party suppliers, to understand where aggregation risk could undermine continuity.

4. Align Minimum Viable Bank priorities with regulatory expectations. Make sure that the identification of core services and dependencies is fully aligned with evolving regulatory standards on resilience.

Third-party vendor management

While financial institutions can outsource business processes, they cannot outsource the risk. Historically, financial institutions have increasingly matured in their third-party risk management, but few have adequate visibility into aggregation risk across fourth- and fifth-party dependencies. These often include cloud providers, SaaS platforms, data vendors, and shared utilities that silently support multiple critical vendors, making them latent systemic risks. In an opaque supply chain landscape, without full insight into vendor dependencies, resilience is only as strong as the weakest link.

- Risk is compounded when multiple vendors rely on the same underlying service (AWS, Akamai, MongoDB, etc.).
- Cascading failures across the vendor ecosystem can create sector-wide outages, especially when concentrated dependencies are unknown.
- Visibility drops dramatically after the 3rd party, most firms do not know who supports their vendors.

Reframe third-party risk as ecosystem fragility and operationalize monitoring beyond the third party.

1. Identify & tag “meta-vendors” (4th-party providers used across multiple 3rd parties).
2. Create a high-risk vendor tier with enhanced oversight, contract terms, and tabletop participation requirements.
3. Mandate disclosure of critical sub-dependencies during procurement and ongoing reviews.
4. Invest in AI-based mapping tools to continuously track changes in extended supply chains.

5. Build a McKinsey-led service offering around Extended Dependency Resilience Mapping.

Companies that proactively map and monitor Nth-party aggregation risk gain a competitive edge in resilience preparedness and can be ahead of evolving regulatory expectations. Generally, regulators hold institutions accountable for all downstream effects: "You own the risk," regardless of which vendor caused the breach.

For McKinsey, this may require a build of a service offering around “Extended Dependency Resilience Mapping,” integrating cyber, ops, and procurement teams to diagnose and mitigate hidden aggregation risk in critical operational service chains.

Comprehensive communications alignment

Resilience is not just about systems, it's about people, language, and coordination. Cyber resilience is often seen as a technological concern, but field evidence suggests that the largest failures during a cyber event arise from organizational communication breakdowns, not the systems themselves. Technical teams often lack clarity on what the business needs in a crisis, and business operations teams lack a common lexicon to translate these core business processes. Generally, these business units are limited in their situational awareness and vocabulary to mitigate human error during cyber events.

- Communication delay is equal to operational delay.
- Misunderstandings can deter decision-making in critical situations.
- Regulators are increasingly looking for integrated responses and are scrutinizing governance, not just controls.

Communication should become a strategic pillar of the resilience strategy.

1. Develop and train on a common lexicon across cyber, ops, legal, and business to reduce “lost in translation” moments during a crisis and build a shared ownership and understanding of resilience response plans.
2. Institutionalize cross-silo tabletop exercises where business, technology, and compliance leaders are in the same room, reacting in real time.

3. Build internal ‘fusion centers’ or integrated response hubs that mirror what successful government models (NCSC, CISA) have done, such as co-locating cyber, ops, and comms teams.

4. Proactively include regulators in non-crisis dialogue to build trust and set disclosure expectations in advance.

Implement a regulatory resilience strategy

Financial institutions must actively foster working relationships with their regulators and fully integrate regulatory engagement into their resilience planning. Firms that operationalize regulatory communication in times of crisis are better positioned to navigate incident response requirements, reduce regulatory friction, and maintain trust with supervisory authorities. This means treating regulators not as after-the-fact audiences, but as key stakeholders in crisis scenarios.

In parallel, institutions should leverage emerging regulatory standards on third-party risk management to demand greater transparency and accountability across their supply chains. Under the EU’s Digital Operational Resilience Act (DORA), European Supervisory Authorities will, by the end of 2025, begin designating “Critical ICT Third-Party Service Providers (CTPPs),” triggering in-depth regulatory assessments of these vendors’ cybersecurity and resilience practices. This oversight creates a valuable opportunity for financial institutions to align their vendor management strategies with regulatory expectations, using these assessments as a basis to negotiate improved access to resilience data and testing cooperation from key suppliers.

Sectoral Deep Dives

Healthcare Sector

"Target rich, resource poor"

Industry Insights

Cyber resilience in healthcare is about maintaining patient care and core operations after an attack.

The healthcare sector operates on razor-thin margins (excluding payers, pharma, and large hospital conglomerates), prioritizes clinical care over cybersecurity, and suffers from fragmented oversight. Its digital dependencies, especially Electronic Health Records (EHRs) and connected medical devices, are critical to care but often poorly understood.

In contrast to other sectors, cyber resilience in healthcare is not just about recovering data or systems; it is about ensuring uninterrupted patient care and maintaining the financial solvency of delivery organizations that rely heavily on digital infrastructure. When systems go down, surgeries are canceled, treatments are delayed, and billing is halted. Resource requirements then rise, pushing some delivery organizations toward insolvency or acquisition which frequently leads to reduction in quality of care. This dual mission to safeguard both clinical operations and financial stability makes healthcare resilience uniquely high stakes, especially with people's lives are directly on the line.

Impact tolerances and digital dependencies are poorly understood

Most healthcare organizations lack a robust understanding of which systems are truly mission-critical and how long operations can withstand digital disruption, such as established “acceptable degraded states” or the minimum viable level of functionality needed to continue safe care delivery based on impact tolerances. How long can these systems be down before care becomes unsafe, or which components must be prioritized for restoration?

For instance, when EHR platforms like Epic is disrupted, surgeries may be postponed, medication orders delayed, and patients put at serious risk. And because Epic integrates with dozens of other systems, from imaging to labs to pharmacy, its failure can trigger a chain reaction of outages across the healthcare delivery system.

The CISO role remains marginalized in healthcare provider settings

Cybersecurity leadership varies dramatically within healthcare providers. While payer organizations (insurance firms) tend to have well-resourced CISOs with executive access, providers, particularly hospitals, often treat the CISO role as peripheral or subordinate.

“CISOs don’t even get board facetime in most hospitals. They’re not valued as much.”

- Healthcare Cybersecurity Expert

Tight margins and competing clinical priorities lead to a culture where security is viewed as a cost, not a mission enabler. A question worth considering posed by another cyber security expert is, “So how much is a CISO worth, day-to-day, compared with a new physician who will allow you to increase your ability to deliver care and allow you to take on more patients to generate income? At what point does that balance change?” Cybersecurity often takes a back seat when healthcare providers are faced with the pressing opportunity to invest in equipment, materials, training, and personnel, which more visibly relate to patient care.

Devices and supply chains create critical weaknesses

The medical device ecosystem is a significant vulnerability. Devices are often running on legacy systems lacking modern security features, not patchable or replaceable without disrupting care, no central entity ensures hospitals apply updates or respond to vendor alerts, and vendors like EPIC or device manufacturers lack the incentive to build in resilience. Similarly, third-party services (billing, claims processing) represent concentrated risk. Amongst 288 CISOs surveyed as part of the 2023 H-ISAC Threat Report, third party and supply chain risk were rated as the third most important threat.[6] The Change Healthcare breach demonstrated how a single vendor failure can paralyze operations across thousands of providers.

Over-reliance on outdated frameworks with fragmented regulatory oversight

Existing standards such as HITRUST, HICP, HPH CPGs are seen as costly, ineffective, and lagging behind threats. For example, UVM Medical Center had implemented 17/20 HPH CPGs in place yet still suffered a ransomware attack that affected patient care for six to nine months.[7] This underscores a critical gap: compliance with frameworks does not guarantee resilience. Compounding the problem is a regulatory landscape where oversight is fragmented across agencies, leaving no single body accountable for ensuring operational continuity in the face of cyber threats. Without realistic testing, redundant systems, or hardened workflows, even the most compliant institutions remain vulnerable to prolonged operational collapse.

Resource constrained

The most vulnerable targets are under-resourced healthcare providers, especially small hospitals in rural areas that often lack dedicated cybersecurity staff or modern infrastructure. Yet, cybersecurity experts agree: more spending does not equal more security. Payer providers are not very vulnerable but not because they are well funded but more so from benefiting from maturity that the financial sector has. They can learn and apply more aptly from fintech and credit card companies' lessons. Without the

[6]2023 H-ISAC Executive Summary Annual Threat Report, Health Information Sharing and Analysis Center, 2023.
[7]Cybersecurity healthcare expert.

expertise to deploy tools effectively or the operational maturity to sustain resilience, increased budgets alone are not a reliable measure of preparedness.

Key Recommendations

To address these challenges, the following strategic levers are recommended:

Reframe cyber resilience as a business continuity issue

1. ***Integrate cyber resilience into enterprise risk management, with explicit accountability at the CEO and board levels*:** The CISO should report to the CEO or COO, not be buried under the CIO, and be evaluated on metrics like patient safety, service continuity, and system uptime.

2. ***Develop dual-path continuity protocols, combining digital restoration plans with offline/manual workflows:*** While digitization has brought major gains, healthcare cannot afford to operate on a "single point of failure" model. Paper-based workflows, offline protocols, and manually executable recovery plans must be developed and maintained, particularly for functions like medication administration, admissions, and emergency care. According to a cybersecurity healthcare expert, "Tech solutions to tech problems don't always work."

3. ***Promote a culture of cyber hygiene by training all healthcare staff, not just IT teams, to recognize threats and respond appropriately*:** Staff are often the first control point and the first vulnerability. Embedding a culture of cyber hygiene through regular staff training ensures that frontline personnel can identify, escalate, and mitigate basic threats before they become systemic failures.

Prioritize resilience over prevention in cyber strategy

1. ***Shift budget and focus on recovery and continuity rather than purely technical prevention*:** Many healthcare organizations are over-indexed on breach prevention, while under-investing in recovery and continuity. That balance must shift. This begins with resource reallocation: funding tabletop exercises, investing in business continuity planning (BCP), and stress-testing degraded operations should receive equal attention to perimeter defenses. As one former

CISO noted, “Most disaster recovery plans are written for auditors, not for real crises.”

In addition, healthcare providers must take a reasonable approach to sourcing and funding cybersecurity improvements. As one healthcare cyber expert notes, “At the individual hospital level, there is no quick fix. It has to be a whole sector approach, part of it starting with its clinical/medical support systems at the hospitals. One of the ways to mitigate the harm to individual hospitals is to ensure the Electronic Record System and medical devices are good.” Therefore, pushing accountability and associated costs upstream to manufacturers can help address systemic vulnerabilities and reduce the burden on individual providers.

Finally, creating clear incentives for hospitals to invest in cybersecurity is essential. Establishing standardized thresholds and categorical benchmarks for CISOs would help prioritize funding, guide resource allocation, and embed resilience as a core operational objective rather than an afterthought.

2. ***Appoint a Chief Resilience Officer and designate a cross-functional Resilience Steering Committee*** to drive this shift that spans IT, clinical, and operational leadership. Resilience must be governed holistically, not in silos.

    - Responsibilities of Chief Resilience Officer: The Chief Resilience Officer is a senior executive responsible for ensuring that the organization can maintain essential functions during and after a cyber disruption. This role is distinct from, but collaborates closely with, the CISO, CIO, COO, and Chief Medical Officer. Think of the CRO as the “Chief of Continuity,” not managing cybersecurity, but ensuring that when systems fail, the hospital still functions. Key responsibilities may include:

        - Define and operationalize “impact tolerance” for clinical services.
            - For example, how long can surgery, emergency care, or medication delivery be delayed before patient harm occurs?
        - Develop, test, and update continuity of operations plans for core services
        - Coordinate resilience investments across departments, ensuring alignment with clinical and operational priorities

    - Serve as a point of integration between IT, clinical operations, facilities, finance, and risk
    - Lead post-incident recovery strategy and cross-functional after-action reviews
    - Report to the CEO or COO and have direct access to the board on resilience metrics and posture

- Composition of Resilience Steering Committee: The Resilience Steering Committee can support the CRO by providing cross-functional input, prioritization, and decision-making across departments. It breaks down silos and ensures that resilience planning reflects the operational reality of the organization. Suggested membership:

    - Chief Resilience Officer (Chair)
    - Chief Information Security Officer (CISO)
    - Chief Operating Officer (COO) or delegate
    - Chief Data Officer
    - Chief Medical Officer or clinical operations lead
    - Head of Facilities/Infrastructure
    - Compliance/Risk Officer
    - External vendors, such as EHR provider reps, managed service providers, are invited quarterly or as needed.

- Mandate of Resilience Steering Committee:

    - Approve and prioritize resilience projects, such as manual fallback development, alternate care routine
    - Oversee annual resilience assessments and simulations
    - Review third-party/vendor continuity guarantees
    - Align resilience goals with regulatory obligations, such as the CMS Emergency Preparedness Rule, HIPAA Security Rule
    - Surface cross-departmental risks and remove institutional blind spots
    - Develop playbooks for degraded operations

3. ***Institutionalize resilience exercises at both the executive and operational levels, including third-party vendors*** **-** Resilience must also be operationalized

through simulation which takes place in advance. Realistic, high-pressure testing, not theoretical runbooks, is what prepares organizations to respond under duress. These exercises should include third-party vendors, who are often tightly integrated into mission-critical workflows but remain outside traditional BCP testing.

Prioritize investments based on risks, vulnerabilities, and impact tolerance

1. ***Conduct cyber impact tolerance assessments to identify "crown jewel" functions*:** Not all systems are equal, but most investment strategies still treat them as such. Cyber funding must be tied to operational criticality and tolerance for disruption. Organizations should conduct impact tolerance assessments to identify "crown jewel" functions, those with high dependency and low tolerance for failure. and ensure they receive priority in recovery sequencing and protection. For example, downtime for trauma surgery systems carries a different risk profile than payroll platforms.

2. ***Adopt a tiered cybersecurity investment model*:** After identifying the crown jewels, healthcare providers should adopt a tiered investment model. For smaller or underfunded organizations, emphasis should be on basic hygiene: strong authentication, backup protocols, endpoint detection. For large health systems, advanced capabilities, such as AI-based analytics, automated threat response, and real-time anomaly detection, should be layered on top of foundational security.

3. ***Enable shared services for resilience*:** The sector needs shared resilience infrastructure. Most rural and under-resourced providers lack the in-house capacity for a full-time CISO or robust resilience program. Shared CISO models, pooled incident response capabilities, and government-supported resilience frameworks (potentially modeled after FEMA or HHS surge teams) can close this gap.

    - ***Shared CISO Services*:** "CISO-as-a-service" model could be offered regionally or through health systems, enabling smaller hospitals to access top-tier strategic cybersecurity leadership without having to fund it alone. A regional healthcare network or a state-supported entity could pool funding

to employ a dedicated CISO team, which serves multiple small hospitals or clinics. These CISOs can provide policy design, regulatory compliance support, vendor security reviews, and incident response leadership.

- ***Regional Incident Response & Resilience Teams*:** A shared technical SWAT team, available across a coalition of providers or under state/federal coordination. These teams would act like cyber EMTs, equipped to deploy quickly when an attack occurs. Services might include immediate containment and forensics, restoration of basic clinical systems, communication coordination with HHS, payers, and regulators. These could be housed within large academic health systems or state health departments and triggered under predefined mutual-aid agreements.

- ***Vendor-Consolidated Resilience Services*:** For hospitals using common platforms, such as Epic and Change Healthcare, resilience services can be coordinated at the vendor level, paid jointly by provider coalitions. Example: a shared backup platform or mirror instance of Epic for a region, activated during ransomware incidents.

Conclusion

The evolving threat landscape has made at least one thing clear: cyber resilience is not optional, it is essential. As cyberattacks grow in frequency, sophistication, and systemic impact, organizations across all sectors must reframe resilience not as a technical safeguard, but as a core operational priority. This means embedding resilience into enterprise risk governance, investing in real-world continuity planning, and holding vendors to higher standards of preparedness. The stakes are no longer limited to data loss or reputational harm; they affect lives, livelihoods, and national stability. Sector-tailored strategies grounded in impact tolerance, extended vendor mapping, and unified leadership are the path forward. The time to act is not after the next breach, but before an organization is tested in crisis.

Key cross-sector takeaways

1. ***Cyberattacks are no longer isolated IT events, they are systemic operational threats*:** Cyber attacks today disrupt not just systems, but services. From hospitals delaying cancer treatments to financial markets halting trades, the impact of cyber events now extends deep into the operational core of critical sectors. These are not rare or theoretical threats, they are frequent, scalable, and increasingly designed to paralyze rather than merely breach. The implication is clear: organizations can no longer afford to view cyber threats purely as technical challenges. The consequences now directly touch patient outcomes, financial solvency, and national security.

2. ***Cyber resilience is about more than just preventing attacks; it must be reframed as a business and mission continuity issue when incidents occur*:** While cybersecurity focuses on prevention, detection, and response, cyber resilience ensures an organization can “handle problems without grinding to a

halt or, to some degree, “gracefully.” Most organizations still treat cybersecurity as an effort to prevent breaches. But in a world where attackers only need to succeed once, the smarter strategy is to assume adverse incidents and prepare for operational continuity during and after an incident. This is the essence of resilience. Resilience must be positioned as a core enterprise risk management concern.

3. ***Current resilience efforts are hampered by governance gaps and outdated assumptions*:** Across all sectors, resilience is fragmented in ownership and often governed by legacy thinking: CISOs are often tasked with resilience but lack operational authority; risk is concentrated in third parties, but few organizations rigorously assess or test vendor resilience; Continuity plans exist, but are often written for compliance, not execution. There is also a deep disconnect between assumed and actual preparedness. Many organizations believe they have continuity plans yet have never run full-scope simulations or mapped dependencies beyond first-tier vendors.

3. ***Third-party dependencies are the Achilles’ heel across all sectors:*** All three sectors struggle with over-reliance on vendors and limited visibility into fourth- and fifth-party dependencies. Attacks like the Change Healthcare breach illustrate how one compromised vendor can cripple an entire sector, especially in healthcare. A key strategy going forward is having an extended dependency resilience mapping which is racking risk beyond direct suppliers.

4. ***Building resilience requires sector-tailored strategies anchored in impact tolerance*:** Resilience is not one-size-fits-all. Each sector, and indeed, each organization, has different thresholds for disruption and different operational realities. Effective resilience requires first identifying which functions matter most, and then ensuring those functions can survive attack or failure. Ultimately, the goal is not to create perfect security but to ensure that when disruptions happen, critical services do not break down.

Key cross-sector recommendations and next steps forward

1. ***Position cyber resilience as a core business risk*:** Integrate resilience into an enterprise risk management, particularly a Chief Resilience Officer (CRO) and

assign board level oversight.

2. ***Establish unified resilience governance:*** Appoint cross-functional leadership with authority over both IT operations and continuity to bridge technical and operational silos.

3. ***Regularly test and exercise continuity plans:*** Conduct full-scope simulations in advance, involving executive leadership and third-party partners to stress-test preparedness.

4. ***Design for failure, not just prevention:*** Identify critical functions and minimal viable operations to ensure that they can continue to operate during and after disruption.

5. ***Hold vendors accountable for resilience:*** Require third parties to demonstrate and test their continuity capabilities. For resource poor organizations, move funding upstream as well as carry out resource pooling when possible. Providers and service operators should advocate for federal oversight, with standardized regulations and guidelines to enforce baseline resilience expectations across the ecosystem.

6. ***Tailor resilience strategies to sector-specific needs:*** Set clear impact tolerance thresholds and adapt resilience strategies to the unique operational demands of each sector.