# Why “Stay Up” Is the New “Stay Safe” in Healthcare Cybersecurity

This article is part of a series expanding on the themes explored in **Executive Brief: The Meditology 2026 Healthcare Security Outlook**. Each installment takes a deeper look at the strategic priorities shaping healthcare cybersecurity in 2026, drawn from executive interviews with CISOs and senior security leaders across the industry.

MEDITOLOGY SERVICES

## EXECUTIVE SUMMARY

- **Metric Shift:** Resilience (downtime) is the new success factor, replacing incident counts.
- **The Goal:** Moving from “Were we breached?” to “Can we still deliver care?”
- **The Bottom Line:** Resilience-oriented projects get funded faster because they protect revenue and patient safety.

Healthcare cybersecurity has been measured by the wrong yardstick for years: incident counts, maturity scores, the number of vulnerabilities patched, etc. These metrics tell leadership whether the security team has been busy, but they say nothing about whether the organization can survive what comes next.

In 2026, that measurement is changing. Across our interviews with CISOs and senior security leaders from some of the nation’s largest health systems, one theme emerged more consistently than any other: **resilience has overtaken prevention as the defining measure of cybersecurity success.**

Boards are no longer asking whether a breach occurred. They are asking how long the organization will be down, whether clinicians can continue delivering care during a disruption, and how quickly critical systems can be restored if a key vendor goes offline. The question has shifted from “Were we breached?” to “Can we still deliver care?”

This is not a subtle language adjustment. It is a fundamental reorientation of what cybersecurity means in a healthcare setting.

# The Catalyst: When Prevention Alone Stopped Being Enough

The shift did not happen in a vacuum. It was accelerated by a series of devastating real-world events that made the consequences of downtime viscerally clear.

Healthcare breaches continued at a brutal pace throughout 2025. More than 700 large breaches were reported to the HHS Office for Civil Rights, and the cumulative toll over the prior two years exposed more than 275 million patient records, a figure that means, statistically, nearly every American has been affected at least once. The average cost of a healthcare breach reached $10.22 million, the highest of any industry for the fourteenth consecutive year.

But the numbers alone did not drive the shift. It was the operational impact that changed the conversation. Ransomware attacks on organizations like Ascension Health, Change Healthcare, and Ardent Health Services did not just steal data, they shut down clinical operations. Emergency departments diverted ambulances. Pharmacies could not dispense medications. Clinicians reverted to paper records while critical systems were rebuilt over days and weeks. In multiple incidents throughout 2025, the ransomware playbook evolved beyond simple encryption: attackers corrupted backups, damaged infrastructure, and compromised clinical systems specifically to prolong downtime and maximize pressure to pay.

As one industry observer noted, attackers are no longer content with stealing data. Their goal is to inflict maximum operational disruption because they understand that healthcare organizations cannot afford to be offline.

When a health system’s ability to deliver care is directly impaired, cybersecurity stops being an IT issue. It becomes a patient safety crisis.

# What Operational Resilience Looks Like in Practice

The CISOs we interviewed described resilience not as a destination but as a journey built on foundational operational discipline. The most mature organizations are approaching it through a structured sequence.

**Start with Critical Business Processes**

Before an organization can be resilient, it must know what it is protecting. The most mature programs begin by mapping their critical business processes, with acute care delivery at the top, and then tracing the technologies, vendor dependencies, and skill sets that support each process. This produces a criticality-based resumption order: if everything goes down simultaneously, what comes back first?

This sounds straightforward, but many health systems discovered during recent disruptions that they had never completed this exercise. As one CISO shared, the organization did not fully appreciate how deeply a single vendor was embedded across care delivery, claims adjudication, and pharmacy operations until that vendor was compromised. Understanding those dependencies in advance rather than during a crisis is the foundation of resilience planning.

**Isolate and Segment**

Several organizations described significant multi-year investments in network segmentation designed so that a compromise at one facility cannot cascade across the enterprise. One health system segmented its entire network to ensure that if a single hospital is attacked, the rest of the organization stays operational. Leaders described this as the "human body" model of resilience: just as the body can quarantine an infection to protect the whole, a well-segmented network contains the blast radius of an attack.

This approach aligns with the broader trajectory of the NIST Cybersecurity Framework 2.0, which emphasizes recovery and resilience alongside its traditional protect-and-detect functions.

HHS reinforced this direction in early 2026 by releasing an updated version of its Risk Identification and Site Criticality (RISC) toolkit, explicitly mapping healthcare facility assessments to both the NIST CSF and HHS Cybersecurity Performance Goals. RISC 2.0 allows organizations to assess the vulnerability of their sites, assess the consequences of disruption, and assess criticality of facilities. The federal signal is clear: resilience is not optional.

> "The first question isn't 'Were we breached?' It's 'Can we still deliver care?'"
>
> — David Finkelstein, St. Luke's University Health Network

**Test with Vendors in the Room**

Tabletop exercises are no longer an internal checkbox. Forward-looking organizations are expanding their resilience simulations to include critical third-party vendors, recognizing that a partner's outage can become a hospital's clinical failure. These exercises test not only technical recovery procedures, but the communication protocols, decision-making chains, and manual workarounds that determine whether care continues when systems are unavailable.

Manual workarounds include reviving the lost art of maintaining paper records and training clinical staff to maintain care standards without digital assistance.

**Change the Metrics**

Mature organizations are replacing traditional security dashboards with resilience-oriented metrics that the board can act on. These

include quantified downtime tolerance (expressed in hours, not abstract risk scores) linked to both financial impact and clinical consequences. When a CISO can tell the board that a ransomware event affecting the EHR will cost a defined amount per day in lost revenue and put specific patient care pathways at risk, the conversation shifts from “Why are we spending this much on security?” to “Are we spending enough?”



## REPLACING TRADITIONAL SECURITY DASHBOARDS

| Traditional Metric (The “Old” Way) | Resilience Metric (The 2026 Way) |
|---|---|
| Number of Vulnerabilities Patched | Recovery Time Objective (RTO) for EHR |
| Phishing Simulation Pass Rates | Duration of Manual Workaround Sustainability |
| Firewall Block Counts | Financial Impact per Hour of Downtime |
| Maturity Scores (NIST/HITRUST) | Vendor Dependency Criticality Map |

# Why Resilience Gets Funded Faster

One of the more striking findings from our research is that resilience-oriented investments are being approved faster than traditional preventive security tooling.

This makes sense when viewed through the lens of healthcare's current financial reality. Organizations operating on razor-thin margins, facing flat or declining security budgets, cannot fund every initiative. When forced to choose, boards gravitate toward investments that directly protect care delivery and reduce the financial exposure of downtime. Disaster recovery modernization, backup environment hardening, network segmentation take begin to take priority over tools that promise to prevent a breach that may or may not occur.

The framing matters enormously. A request for a new threat intelligence platform is an IT expenditure. A request to reduce the organization's recovery time from 14 days to 48 hours after a ransomware attack is a business continuity investment that protects revenue, reputation, and patient safety. Both may be worth funding, but the second one speaks the board's language.

# The Road Ahead

Operational resilience is not a project with a completion date. It is an operating model. It's a continuous cycle of identifying critical processes, testing recovery capabilities, incorporating lessons learned, and adapting to an evolving threat landscape.

Healthcare organizations that embrace this shift will find themselves better positioned not only to survive cyberattacks, but to maintain the trust of the patients, clinicians, and communities they serve. Those that continue to measure success solely by whether a breach occurred will be caught flat-footed when the inevitable happens.

The threat actors are aware healthcare organizations cannot afford downtime. The question for 2026 is whether healthcare security leaders are prepared for the evolving threat landscape.

See the following Healthcare Operational Resilience Checklist to see how ready you are.



# Healthcare Operational Resilience Checklist

| 1. Critical Process & Dependency Mapping | 2. Architectural Isolation (Containment) | 3. Third-Party & Vendor Integration | 4. Operational & Manual Readiness | 5. Board Reporting & Financial Alignment |
|---|---|---|---|---|
| **Identify Core Missions:** Define and rank critical business processes, placing acute care delivery at the top of the hierarchy. | **Implement Enterprise Segmentation:** Invest in network segmentation to ensure a compromise at one facility cannot cascade across the entire enterprise. | **Expand Tabletop Exercises:** Include critical third-party vendors in simulation exercises to test shared response capabilities. | **Validate Manual Workarounds:** Test the clinical staff's ability to maintain patient care through manual workarounds when digital systems are unavailable. | **Quantify Downtime Tolerance:** Define recovery time objectives (RTO) in hours rather than abstract risk scores. |
| **Trace Technical Dependencies:** Map the specific technologies, vendor integrations, and internal skill sets required to support each critical process. | **Adopt the "Human Body" Model:** Design the network to quarantine infections/attacks locally to protect the functionality of the whole organization. | **Verify Communication Protocols:** Document and test the specific communication chains and decision-making protocols used when a vendor goes offline. | **Harden Recovery Environments:** Modernize disaster recovery and ensure backup environments are hardened against encryption or corruption. | **Translate Risk to Revenue:** Tie downtime metrics directly to lost revenue per day and specific patient care pathway risks. |
| **Define Resumption Order:** Establish a documented, criticality-based resumption order to determine which systems are restored first during a total outage. | **Limit "Blast Radius":** Validate that a ransomware event in one segment is technically isolated from clinical or financial segments. | **Assess Site Criticality:** Utilize the HHS Risk Identification and Site Criticality (RISC) toolkit to map facility assessments to federal performance goals. | **Review Regulatory Readiness:** Ensure resilience planning meets evolving federal signals and HHS Cybersecurity Performance Goals. | **Frame as Business Continuity:** Present resilience requests as business continuity investments (protecting reputation and safety) rather than IT expenditures. |
| **Uncover "Invisible" Dependencies:** Identify single points of failure where a single vendor may be embedded across care delivery, claims, and pharmacy operations. | **Align with NIST CSF 2.0:** Ensure the security architecture emphasizes recovery and resilience functions alongside traditional protection. | **Evaluate Supply Chain Resilience:** Shift from reactive vendor assessments to proactive architectural risk reviews and continuous monitoring. | | **Focus on Impact over Incidents:** Shift board reporting from "incident counts" to the organization's ability to survive and deliver care during a disruption. |

# About Meditology Services and this Research

Meditology Services is a healthcare-exclusive cybersecurity advisory firm. As the facilitator of this research and a trusted partner to hundreds of healthcare organizations nationwide, Meditology translates peer insights into actionable programs that accelerate security program maturity.

To execute on the strategic priorities outlined in this report, Meditology partners with healthcare organizations across critical areas:



### Operationalize Resilience & Third-Party Risk (TPRM)

Transition from reactive vendor assessment to proactive supply chain resilience through architectural risk reviews, continuous monitoring, and vendor integration into business continuity planning.



### Achieve Industry-Standard Certifications

Pursue HITRUST certifications and SOC 2 attestations to provide validated proof of security maturity to partners, patients, and regulators.



### Validate Security Through Continuous Technical Testing

Replace point-in-time assessments with continuous testing and ethical hacking to ensure controls remain effective against an evolving threat landscape.



### Establish AI & Emerging Technology Governance

Proactively manage the risks of AI adoption through AI risk program and governance frameworks that ensure innovation does not outpace security.

**This executive report is based on in-depth executive interviews conducted during January and February 2026** with CISOs and senior cybersecurity leaders representing multi-state integrated delivery networks, academic medical centers, regional and community health systems, health plans, and health technology companies.

Discussion areas included enterprise risk prioritization, budget strategy, vendor governance, security operations, regulatory readiness, and emerging technology risk. All findings are reinforced by Meditology's proprietary data derived from hundreds of healthcare cybersecurity engagements conducted annually.

**Participants included:**

- Gillian Lockwood, Director, Information Security, Mass General Brigham
- Matthew Webb, AVP, Cyber Risk Management, HCA
- Zishan Siddiqui, CISO, Sentara Health
- David Finklestein, CISO, St. Luke's University Health Network
- Raj Raju, CISO, Integra Connect
- Denis Tanguay, CIO, Sturdy Health
- Paul Curylo, CISO, Inova Health System
- Among others who requested anonymity.

All insights are presented in aggregate to reflect industry-wide themes rather than the position of any single organization.

## About This Series

*This article is the first in a series of deep dives from the* **Executive Summary Brief: The Meditology 2026 Healthcare Security Outlook**. *Upcoming installments will explore modernizing third-party risk management, building AI governance frameworks, and operationalizing GRC programs for healthcare.*

MEDITOLOGY SERVICES

For more information, visit **www.meditologyservices.com** or contact your Meditology engagement team.

© 2026 Meditology Services, LLC. All Rights Reserved