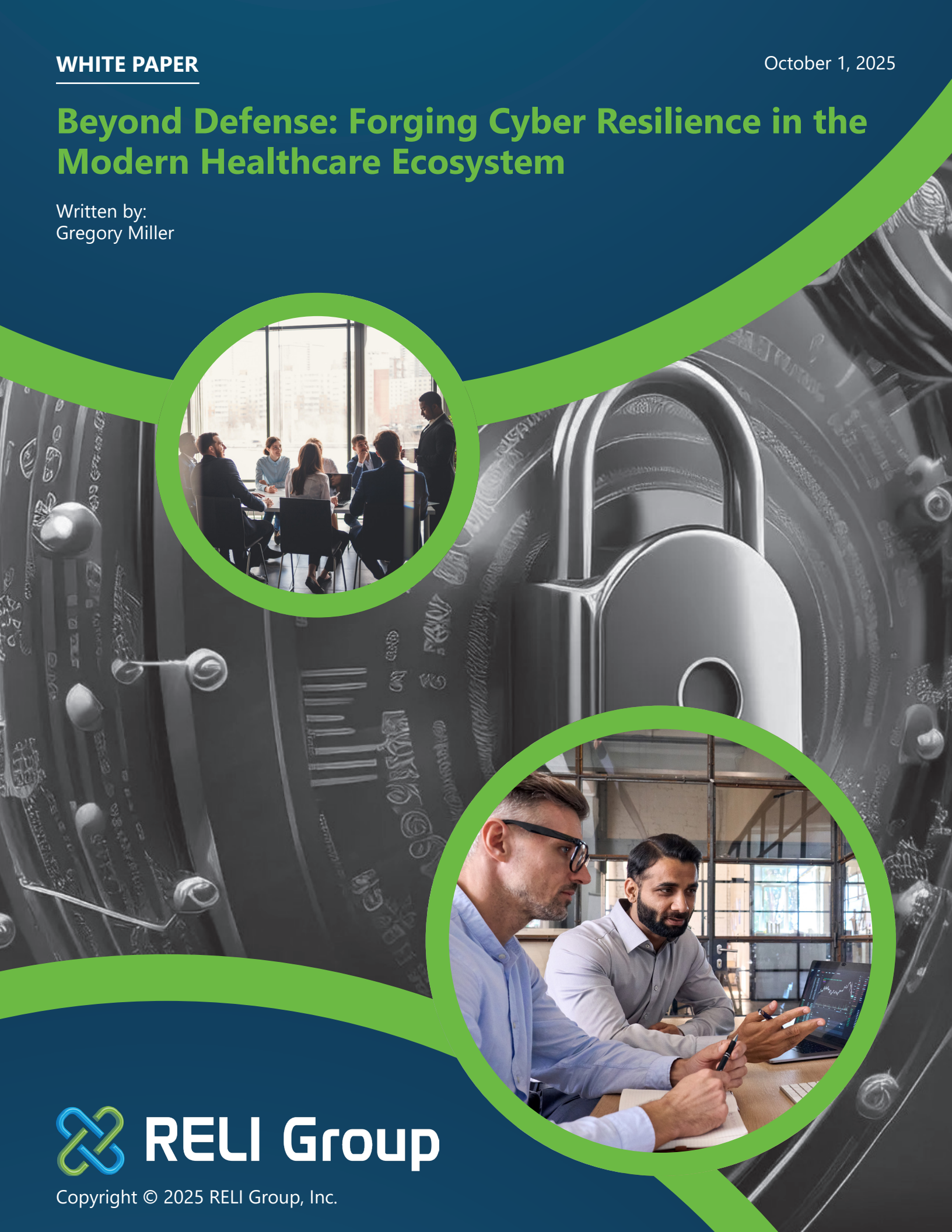
WHITE PAPER

October 1, 2025

Beyond Defense: Forging Cyber Resilience in the Modern Healthcare Ecosystem

Written by:
Gregory Miller



RELI Group

RELI Group

Beyond Defense: Forging Cyber Resilience in the Modern Healthcare Ecosystem

The healthcare industry has become one of the most heavily targeted sectors for cyberattacks, facing threats that extend far beyond data theft to full-scale operational disruption. With breaches in recent years exposing hundreds of millions of patient records and incidents like the Change Healthcare ransomware attack crippling core functions of the U.S. medical system, the urgency for stronger protections has never been greater. Traditional defensive measures alone are no longer sufficient in such a dynamic threat landscape. Instead, organizations must adopt a mindset of cyber resilience – one that emphasizes anticipating, withstanding and rapidly recovering from attacks while ensuring the continuity of patient care. This paper explores the evolving cyber threat environment; outlines a framework for building resilience through intelligence, governance and secure design; and highlights how proven expertise in complex healthcare ecosystems can serve as a model for organizations seeking to protect both their operations and the patients they serve.

The healthcare industry is facing a cybersecurity crisis of unprecedented scale. According to a year-end analysis of federal data by The HIPAA Journal, the sector witnessed a record number of large-scale data breaches in 2023, exposing the sensitive records of more than 133 million individuals. The crisis deepened further in 2024, with breaches compromising over 278 million records – more than doubling the previous year's total. This surge was driven in part by catastrophic incidents such as the Change Healthcare ransomware attack, which alone impacted an estimated 190 million people, making 2024 the most devastating year on record for healthcare data security. This staggering figure, which represents a 139 percent increase from the previous year, is corroborated by other industry analyses, such as the 2024 Horizon Report from Fortified Health Security. These are not mere statistics; they are official figures compiled from data reported directly to the U.S. Department of Health & Human Services Office for Civil Rights, representing a fundamental threat to patient safety, privacy, and the operational stability of healthcare organizations.

The Change Healthcare ransomware attack alone impacted an estimated 190 million people, making 2024 the most devastating year on record for healthcare data security.

The vulnerability of the U.S. healthcare system to cyberattacks was laid bare in early 2024 by the catastrophic ransomware attack on Change Healthcare. This single incident not only breached data but also paralyzed a system responsible for processing half of all U.S. medical claims, halting prescription fulfillment for patients and crippling the revenue streams of thousands of providers nationwide. This event serves as a stark illustration that the primary threat has evolved beyond data loss to complete operational failure.

RELI Group

Beyond Defense: Forging Cyber Resilience in the Modern Healthcare Ecosystem

Cyber adversaries target healthcare for a simple reason: the value of the data and the critical nature of the services provided. Protected Health Information (PHI) is a highly valuable commodity on the dark web, and the potential for ransomware to disrupt lifesaving operations creates immense leverage for attackers. The consequences of a successful breach extend far beyond financial penalties under regulations like the Health Insurance Portability and Accountability Act (HIPAA). They include:

- **Medical System Collapse.** A cyberattack could disable or destroy essential administrative and clinical systems, disrupting patient care and the ecosystem's ability to function.
- **Disruption of Patient Care.** Canceled appointments, delayed surgeries and inaccessible patient records can have life-threatening consequences.
- **Erosion of Public Trust.** Patients must feel confident that their most sensitive data is secure. A breach shatters this trust, causing lasting reputational damage.

In a data-rich environment, a traditional, defensive cybersecurity posture is no longer sufficient. The modern, interconnected healthcare ecosystem, including hospitals, clinics, insurers and a myriad of technology partners, has too many entry points for a purely preventative strategy to be foolproof. The critical question is not if your organization will be targeted, but when.

The critical question is not if your organization will be targeted, but when.

The necessary evolution is a shift in mindset from cybersecurity to cyber resilience. Resilience is the ability to anticipate, withstand, recover from and adapt to adverse cyber events. It's a proactive strategy focused on building agility into operations to quickly identify, address, remediate and recover from an incident, often without impacting the core mission of patient care.

The Evolving Threat Landscape

Today's threats are dynamic and multifaceted, rendering legacy security models obsolete. Healthcare organizations must contend with:

- **Sophisticated Ransomware.** Attackers now exfiltrate data before encrypting it, adding the threat of public exposure to operational disruption.
- **Targeted Phishing and Social Engineering.** Exploiting the human element remains a primary vector for initial access.
- **Vulnerabilities in Interconnected Systems.** The proliferation of Internet of Things medical devices, third-party vendor systems and cloud-based electronic health records expands the attack surface exponentially.

True resilience requires a framework that acknowledges these realities – a framework built not on impenetrable walls, but on the capacity to see, understand and respond to threats with speed and precision.

RELI Group

Beyond Defense: Forging Cyber Resilience in the Modern Healthcare Ecosystem

A Framework for Cyber Resilience: From Compliance to Operational Readiness

Achieving cyber resilience requires a deliberate, multi-layered strategy that integrates people, processes and technology. It's about building a security-aware culture and embedding resilience into the organization's very fabric. This framework is built on three core pillars.

Pillar 1: Agile Threat Intelligence and Response

Organizations must move beyond static defenses and adopt a dynamic, proactive approach to threat management. This includes:

- **Proactive Threat Hunting:** Searching for indicators of compromise and anomalies in real time, enhanced by AI/ML analytics.
- **Trend Identification:** Using predictive analytics and intelligence feeds to forecast threats before they materialize.
- **Rapid Response and Containment:** Executing rehearsed, AI-enabled response plans to isolate, neutralize and recover from incidents quickly.

Pillar 2: Integrated Governance, Risk, and Compliance (GRC)

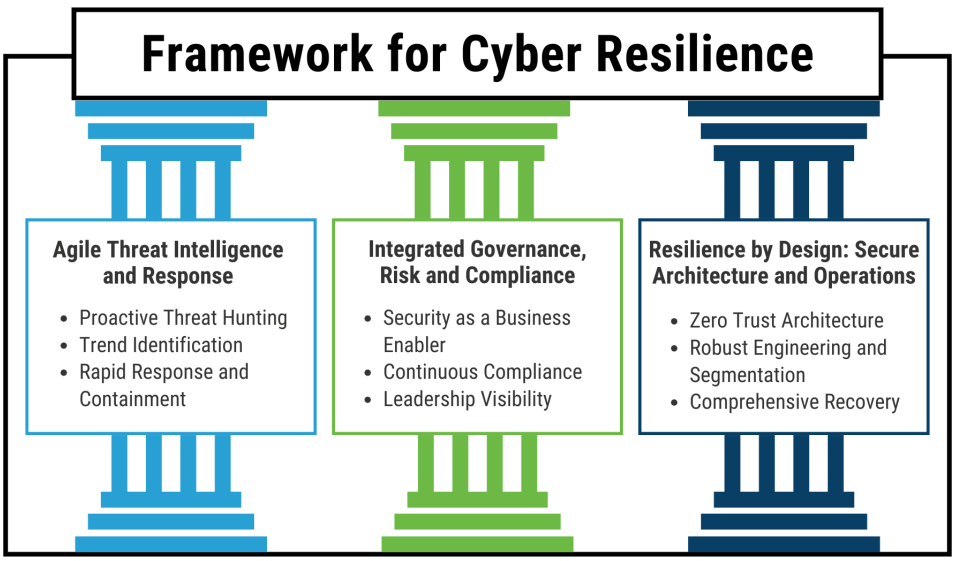
Compliance serves as the foundation for resilience, ensuring risk management and security align with business priorities. This pillar emphasizes:

- **Security as a Business Enabler:** Embedding risk considerations into strategic and operational decision-making.
- **Continuous Compliance:** Maintaining audit readiness and adapting rapidly to evolving regulatory requirements with AI-driven monitoring.
- **Leadership Visibility:** Delivering accurate, timely insights so executives can make informed, risk-based security investments.

Pillar 3: Resilience by Design – Secure Architecture and Operations

Resilience must be built into the fabric of systems and workflows from the outset. This includes:

- **Zero Trust Architecture:** Enforcing the principle of "never trust, always verify" to limit lateral movement.
- **Robust Engineering and Segmentation:** Designing networks that isolate critical assets and contain impact.
- **Comprehensive Recovery Plans:** Maintaining reliable, tested data backup and disaster recovery processes for rapid restoration.



RELI Group

Beyond Defense: Forging Cyber Resilience in the Modern Healthcare Ecosystem

Case Study: Lessons from Federal Healthcare Cybersecurity

Translating this framework from theory to practice requires experience operating at scale. One example comes from RELI Group's work on the Marketplace Security Services Privacy Support Services (MSSPSS) contract for the Centers for Medicare & Medicaid Services (CMS).

This vital contract ensures the security and privacy of the Affordable Care Act infrastructure, a vast, interconnected ecosystem comprising state-based exchanges, federally facilitated exchanges, Medicaid agencies, and commercial partners such as web brokers and enhanced direct enrollment entities. In this complex environment, RELI provides the foundational cybersecurity services that enable CMS leadership to protect the sensitive information of millions of Americans and ensure the integrity of the nation's health insurance marketplace.

RELI's experience on the MSSPSS contract is not just a credential; it is a direct blueprint for how healthcare organizations can achieve cyber resilience. Our comprehensive services map directly to the pillars of a modern, resilient security program.

RELI's experience on the MSSPSS contract is not just a credential; it is a direct blueprint for how healthcare organizations can achieve cyber resilience.

Leveraging Proven Federal Experience for Your Organization

The challenges of securing a national healthcare marketplace are directly applicable to any healthcare organization. Through our work on the MSSPSS contract, we have identified several practices that can help healthcare entities strengthen their cybersecurity posture, including:

- **Cybersecurity Program Management and Oversight.** We establish the strategic planning and risk management functions essential for a mature security program.
- **Governance, Risk, and Compliance Support.** We are experts in navigating the complex regulatory landscape of FISMA, HIPAA and the NIST RMF, ensuring compliance is a continuous and integrated process.
- **Security Architecture and Engineering Guidance.** Our team provides the strategic direction needed to build resilience by design, ensuring systems are secure from their inception.
- **Security Assessment & Authorization (SA&A).** We implement rigorous assessment processes that validate security controls and ensure system integrity before and during operation. We also leverage AI and automation tools to analyze large datasets and streamline documentation, accelerating the SA&A process and allowing our experts to focus on complex, high-risk areas.

For CMS, we provide complete, accurate and timely information that C-level executives need to make critical, risk-based decisions. We bring that same level of clarity and strategic insight to our commercial healthcare partners.

The Next Frontier: Integrating Digital Forensics to Enhance Resilience

As RELI expands its digital forensics capabilities within the MSSPSS contract, we are introducing a powerful new tool to support the healthcare mission. This expertise moves beyond post-incident analysis to become a proactive component of resilience:

- **Deeper Threat Understanding.** Forensics uncovers the specific tactics, techniques and procedures used by adversaries, allowing for more effective, targeted defenses.
- **Enhanced Trend Analysis.** By forensically analyzing low-level security events, we can identify trends that reveal sophisticated, malicious intent long before a significant incident occurs.
- **Smarter Remediation and Recovery:** Understanding the precise root cause and extent of a compromise enables faster, more complete remediation and a more robust recovery, preventing reinfection.

This forensic-informed approach strengthens the entire resilience lifecycle, from identifying emerging threats to ensuring a full recovery – ultimately protecting the core mission of delivering patient care.

Building Toward Cyber Resilience

The healthcare industry is at a critical inflection point. The escalating volume and sophistication of cyber threats demand a fundamental shift from a defensive posture to a proactive strategy of cyber resilience. Compliance provides an important baseline, but true resilience goes further: anticipating threats, embedding secure design into systems, and cultivating a culture of preparedness.

Federal initiatives such as CMS' marketplace security program demonstrate how resilience frameworks can be implemented in complex, data-rich environments. Through its role on the MSSPSS contract, RELI Group has contributed to shaping and executing these resilience strategies at a national level. The insights gained from this work highlight practical steps any healthcare organization can take to protect patient safety, maintain trust, and ensure continuity of care in the face of persistent threats.

References

Beyond Defense: Forging Cyber Resilience in the Modern Healthcare Ecosystem. (n.d.).

The New Frontline: A Healthcare System Under Siege. (n.d.).

Fortified Health Security. (2024). 2024 Horizon Report.

The HIPAA Journal. (2024). 2023 Healthcare Data Breach Report.

National Institute of Standards and Technology (NIST). (n.d.). Risk Management Framework (RMF).

U.S. Department of Health and Human Services (HHS) Office for Civil Rights. (n.d.).

Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073.

Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.