Protecting What Truly Matters

A Leadership Blueprint for Healthcare Cybersecurity

By Jericho Simmons
Shield and Seed LLC

Executive Summary

The healthcare sector is facing a turning point. There are fewer reported breaches in 2025, yet the financial and operational impact of cyber incidents continues to rise. This article outlines why alignment between executives and security leaders is essential for effective protection, identifies the business functions that must be prioritized, and explains how a clarity-driven approach grounded in stewardship can transform cybersecurity into a leadership discipline that strengthens resilience and safeguards what matters most.

Introduction

As of December 3, 2025, the OCR reports 561 healthcare breaches involving 500 or more patient records, exposing more than 34 million individuals. IBM's 2025 Cost of a Data Breach Report provides additional context. Although the global average breach cost decreased slightly to 4.44 million dollars, the United States average increased to 10.22 million dollars. Verizon's DBIR highlights that ransomware appears in 44 percent of breaches and that healthcare remains the most affected industry, with 1,542 confirmed incidents.

These figures reflect more than technical vulnerabilities. They reveal an ongoing leadership challenge. Compared to 742 healthcare incidents in 2024, this year represents a 24 percent decline. The question is whether this reflects fewer attacks or increased maturity in detection, reporting, and defensive posture. Understanding this shift requires a change in mindset from urgency based reaction to intentional, expectation aligned stewardship.

The Changing Breach Landscape

Looking back over the past decade, 2025 is the first significant decline in reported healthcare breaches in five years. While December may adjust the final numbers, the downward trend is notable.

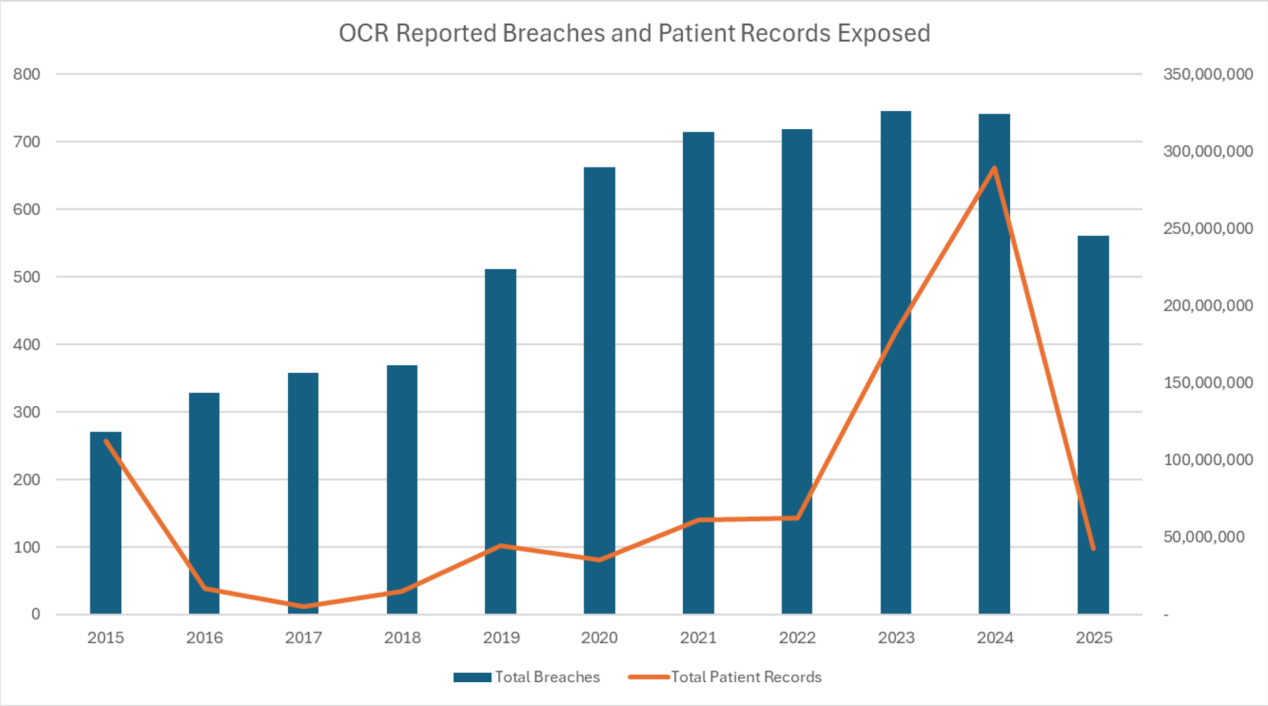


Figure 1. OCR-Reported Healthcare Breaches and Patient Records Exposed (2015–2025)
This chart highlights a steady rise in healthcare breaches over the last decade, followed by the first meaningful decline in 2025. While breach counts decreased, the number of patient records exposed remained highly volatile, with 2024 showing a significant spike. This reinforces that fewer incidents does not always mean reduced impact. The data emphasizes the importance of leadership clarity in interpreting risk trends rather than relying solely on breach volume.

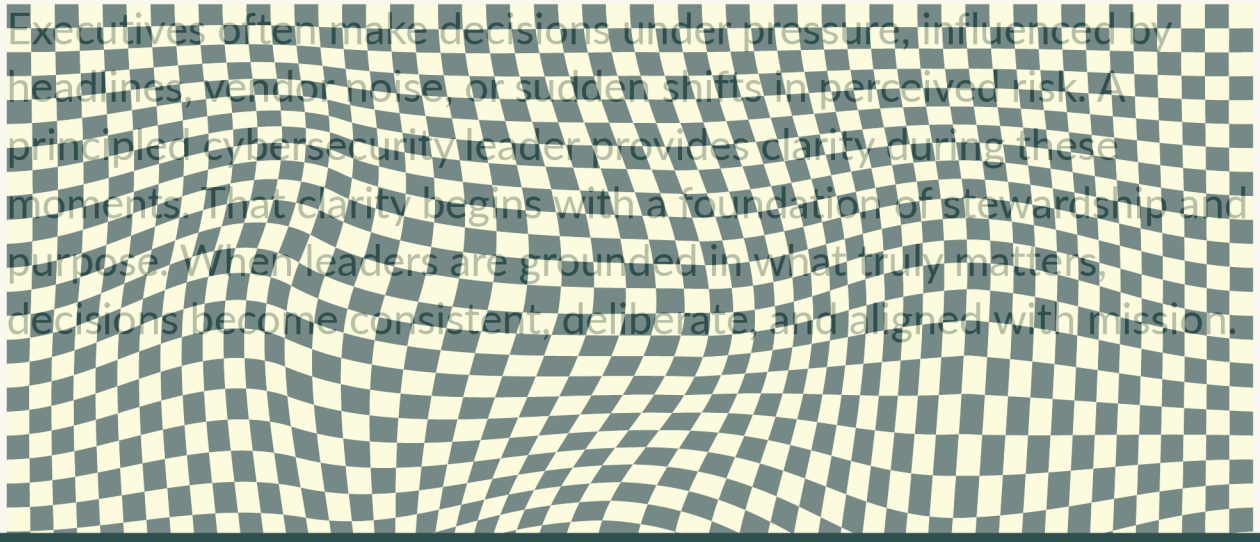
This improvement likely comes from several factors:

- Security tools that now incorporate more capable and mature AI models
- Increased workforce skill and improved response processes
- Better integration between security teams and operational leaders
- A broader awareness of cyber risk across healthcare

IBM reports a seven year low in both time to identify a breach at 181 days and time to contain a breach at 60 days. While 241 days of dwell time is far from ideal, the trend suggests growing maturity. Yet even these improvements highlight an ongoing tension. Organizations often expect outcomes that do not match the realities shown in the data. This disconnect leads to reactive efforts rather than clear, well aligned strategies.

Cybersecurity leadership requires executives and technical teams to share a unified understanding of what “good” performance looks like and how it should be measured.

The Leadership Imperative: Aligning on What Matters Most



Security is strongest when leaders:

- Define acceptable risk
- Set clear expectations
- Align protective actions with organizational purpose
- Prioritize based on business function, not fear

Baseline data from IBM and Verizon can guide decisions, but they are starting points. Each healthcare organization must interpret risk in the context of its people, its operations, and the mission it preserves.

Ransomware continues to be the most likely and most disruptive event. Yet even this does not fully answer the question of what must be protected first.

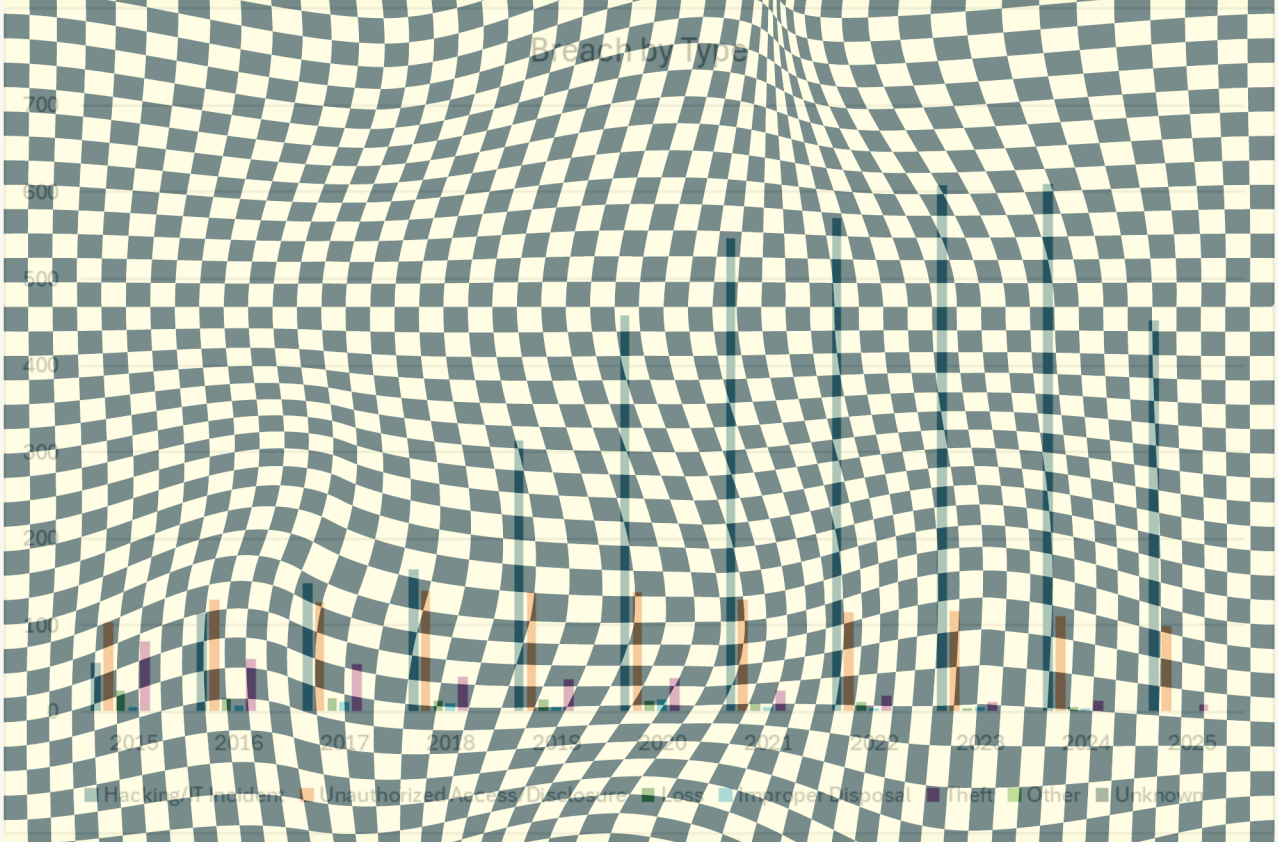


Figure 2: Healthcare Breaches by Type Over Time
Hacking and IT-related incidents have grown dramatically across the past decade and now represent the vast majority of healthcare breaches. This shift confirms that modern cyber threats are increasingly targeted, sophisticated, and financially motivated. The data demonstrates why executive alignment around prevention, rapid detection, and impact reduction is essential for protecting the functions that sustain patient care and organizational mission.

To clarify priorities, I use a simple leadership model:

1. Prevent incidents where possible
2. Respond quickly when they occur
3. Reduce impact by limiting what attackers can access or disrupt

This model keeps communication clear and ensures that security strategies can be understood at every level of leadership.

Risk Must Begin With the Business

Security professionals can identify technical vulnerabilities with ease, but that perspective is not enough. True prioritization begins with the board and senior executives. Leaders must articulate what loss the organization can tolerate, how long they can withstand downtime, and which functions are essential to protect first.

This ties directly to a fundamental principle of security stewardship: the hierarchy of importance.

1. People
2. Community and mission
3. Business operations

Human life and patient safety always come first. A person's well-being is far more important than reclaiming one percent of lost claims. This hierarchy shapes how we think about breaches, response readiness, and organizational priorities.

Expanding Beyond Revenue Cycle: What Else Must Be Protected

Revenue cycle is a clear example of how operational disruption creates significant financial consequences. However, it is only one part of a broader ecosystem. To protect an organization effectively, leaders must assess all critical functions that sustain patient care, maintain regulatory compliance, and support financial stability.

1. Clinical Operations

- Electronic health records
- Clinical documentation
- Medication management
- Imaging and laboratory systems
- Scheduling and care coordination

Disruption in these areas directly affects patient safety, which sits at the top of the hierarchy.

2. Revenue Cycle (Beyond Finance)

Revenue cycle extends across multiple departments:

- Patient access and registration
- Eligibility and benefits verification
- Coding and documentation
- Clinical documentation integrity
- Claims submission and reimbursement
- Denial management

These interconnected workflows rely on accurate clinical information and stable technology. Their disruption affects cash

flow, margins, and long term financial health.

3. Supply Chain and Logistics

- Medication and device procurement
- Inventory tracking
- Distribution workflows
- Vendor dependencies

If these functions fail, patient care is immediately impacted.

4. Enterprise IT and Shared Services

- Identity and access management
- Network infrastructure
- Communication systems
- Backup and recovery capabilities

These functions determine how quickly the organization can adapt during a crisis.

5. Administrative, Quality, and Regulatory Functions

- Compliance reporting
- Risk management
- Human resources and workforce systems

These areas carry high regulatory and operational significance.

Protecting these functions requires a holistic view of the organization. Security becomes a partner in enabling mission, protecting people, and supporting the business entrusted to the leadership team.

Why This Matters

The goal is not to protect every system equally. It is to identify which functions sustain life, care delivery, and organizational mission. Revenue cycle illustrates the financial dimension, but every critical function must be evaluated through the same lens.

This shift moves healthcare cybersecurity from a system centered mindset to a purpose centered one. It recognizes that security is not just a technical responsibility. It is a leadership responsibility grounded in alignment, stewardship, and clarity.

Conclusion

Data is an essential tool for cybersecurity, not only in a technical sense but also as a source of business insight. When cybersecurity leaders understand operational workflows, financial drivers, and the mission of the organization, they become strategic partners who strengthen resilience and protect what matters most.

Ransomware and operational disruption will remain significant threats, but with alignment, clarity, and purpose driven leadership, security can shift from reactive firefighting to a discipline rooted in stewardship and long term value.

Call to Action

If your organization is ready to move beyond reactive cybersecurity and build a security program aligned with what matters most, Shield and Seed is here to help. We partner with healthcare leaders to bring clarity to decision making, identify critical functions, and build practical strategies that strengthen resilience.

Start the conversation today. Visit Shield and Seed to explore cybersecurity consulting, executive mentorship, and strategic planning that aligns with your mission and your future.

Secure the present. Sow the future.

Sources:
https://marketplace.optum.com/content/dam/change-healthcare/marketplace-assets/outcomes-and-insights/2024-denials-index.pdf
https://www.law.cornell.edu/regulations/texas/1-Tex-Admin-Code-SS-354-1003
2025-dbir-data-breach-investigations-report.pdf
cost-of-a-data-breach-2025-full-report.pdf

About the Author

Jericho Simmons is a healthcare cybersecurity executive with more than a decade of experience leading security strategy, operations, and risk programs across complex healthcare environments. His leadership approach is grounded in clarity, stewardship, and a deep commitment to protecting what sustains patient care and organizational mission.

Jericho specializes in aligning cybersecurity with clinical operations, revenue cycle performance, and executive decision making. Through Shield and Seed, he partners with healthcare leaders to build purpose-driven, business-aligned security strategies that strengthen resilience, reduce risk, and support long term organizational health.

Jericho Simmons
Technology Executive
jericho.simmons@shieldandseed.net
www.shieldandseed.net

SHIELD & Seed LLC
SECURE THE PRESENT. SOW THE FUTURE.