

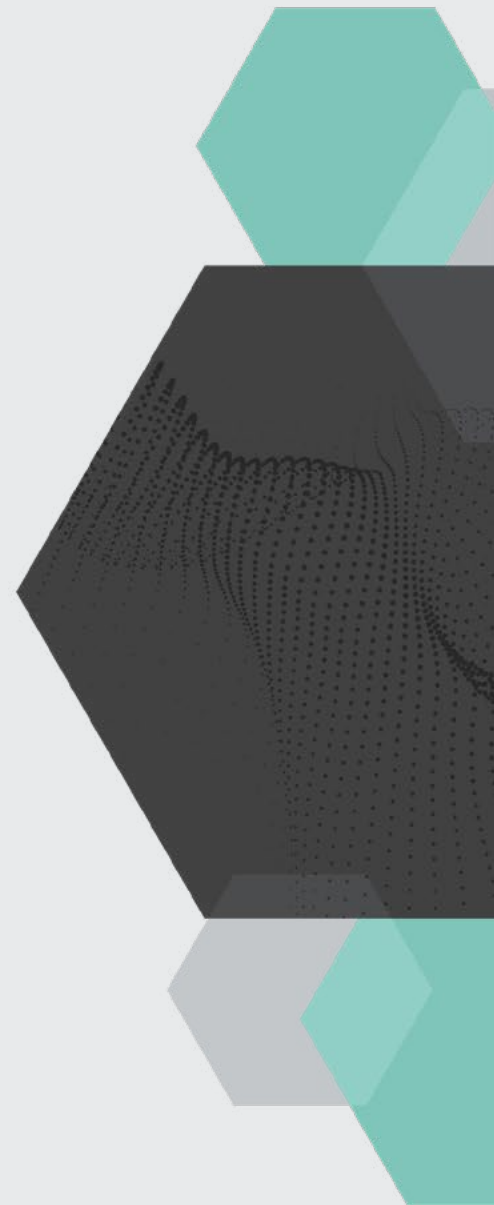


# 2025 HORIZON REPORT

The state of cybersecurity in healthcare

# Contents

- 01 CEO Message
- 02 2024 Year in Review
- 08 Prioritizing Healthcare Cybersecurity on a Tight Budget
- 14 Communicating With Your Board: Telling Your Story and Using Metrics That Matter
- 18 The Future of Healthcare Cybersecurity Legislation: A Collective Push Toward Resilience
- 24 AI in Healthcare Cybersecurity: A Double-Edged Sword Shaping the Future of Hospitals
- 30 Threat Actor Evolution in Healthcare Cybersecurity
- 34 Advancing Third-Party Risk Management in Healthcare
- 38 2025 Cybersecurity Predictions
- 42 About the Contributors



# CEO's Message

As we enter 2025, the healthcare sector will be confronted with a rise in cyberattacks, strict legislative regulations, and the ongoing enhancement of AI, all while navigating financial pressures.

There are no "one-size-fits-all" answers to confronting these challenges. That is why collaboration is critical to safeguarding cybersecurity risks. By continuing to strengthen and expand our partnerships across the healthcare ecosystem -- from payers to providers to technology companies to biotech -- we enhance our resources and expertise. This is how we help you respond even more effectively to breaches, stay ahead of threats, and meet new regulatory requirements.


Fortified's trusted team of industry experts, featured in this Horizon Report, actively engages year-round in cybersecurity discussions through roundtables, webinars, panels, and advisory committees. They are dedicated to gathering new insights and best practices, empowering us to problem-solve as a unified, collaborative community.

Let's use these collaborative efforts to advance enhanced security, tailored solutions, and efficient compliance and risk management. Let's strengthen staff training, perform continuous security assessments, and improve incident response, so all healthcare organizations can possess a resilient defense system to tackle emerging threats.

At Fortified Health Security, we are referred to as "Healthcare's Cybersecurity Partner" because we know partnerships are the key to success. Looking ahead, we remain dedicated to continuing our collaboration with the entire healthcare industry and sharing our solutions to protect your data and patient lives.

Together, we can secure the future of healthcare and safeguard patient trust.

Warm regards,



Dan L. Dodson



2025 Horizon Report | 02

# 2024 Year in Review

## Fewer Breaches, Greater Impact.

In 2024, while the number of cybersecurity breaches decreased 7% year over year, their impact grew significantly. In fact, more than 15 million additional patients were affected by breaches than in 2023.

Cybercriminals are becoming more sophisticated, exploiting new threat vectors such as third-party vendors, and employing advanced techniques. These attacks are no longer just about stealing data—they're disrupting and even shutting down entire healthcare operations.

Mitigating these complex threats requires investment in cybersecurity personnel and defense systems. However, budget constraints and a growing talent gap

make it increasingly challenging to safeguard patients and healthcare organizations.

There are actionable solutions outlined throughout the Horizon Report to address these complex threats. But to mitigate or remediate these threats we must start with a clear view and understanding of the data from the 2024 key breaches.

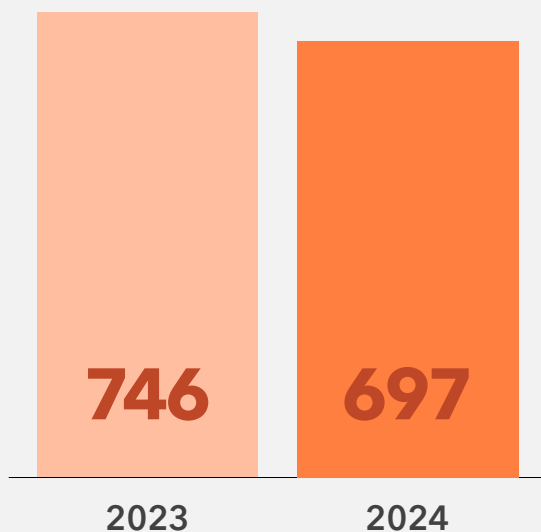
The following should serve as a wake-up call across the continuum of healthcare. But there are actionable solutions we've outlined throughout this Horizon Report, let's start with a clear view of where the vulnerabilities lie.

## Number of Breaches and Patient Records Exposed

The total number of patient records exposed in 2024 rose 9%, reaching more than 183 million. This increase highlights the growing impact of large-scale breaches. Business Associates played a significant role, accounting for 67% of exposed records, a 6% increase YoY, while Healthcare providers exposed records dropped by 6 points.

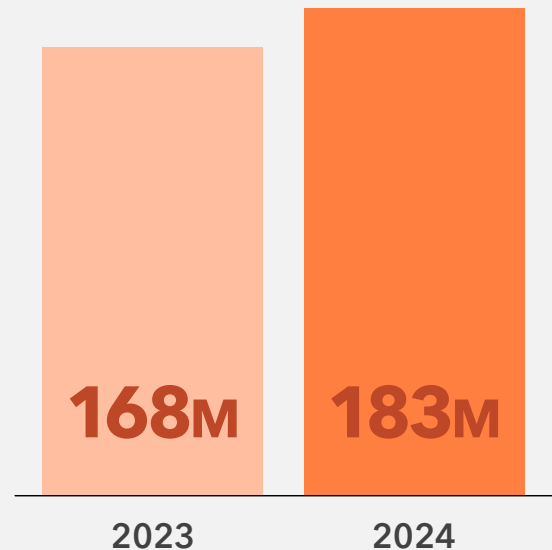
### Breaches

2023 vs 2024



### Patient records exposed

2023 vs 2024



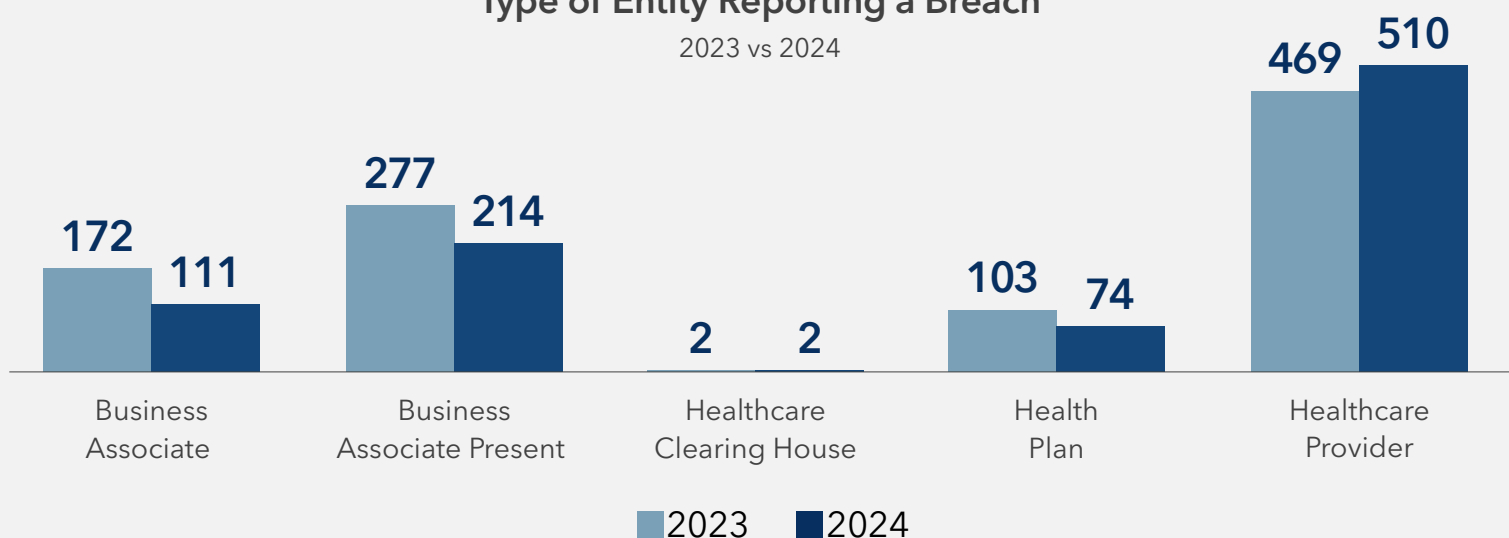
# Type of Entity Reporting a Breach 2023 vs 2024

Business Associates continued to lead as the largest contributors to breaches, yet Health Clearing Houses saw an alarming 2453% year-over-year increase in exposed records. This sharp rise highlights the growing vulnerability of entities that manage massive volumes of sensitive patient data and critical healthcare services.

Healthcare leaders need to prioritize securing these high-risk entities. Strengthening protections and ensuring compliance with evolving cybersecurity standards is no longer optional - it's essential to mitigating risks and maintaining trust in the healthcare ecosystem.

## Type of Entity Reporting a Breach

2023 vs 2024



## Entity Type Definitions

- » **Business Associate**  
Person or organization that performs a function or activity on behalf of a covered entity but is not part of the covered entity's workforce. Can also be a covered entity. BAs can be the source of the breach or part of it ("BA Present").
- » **Healthcare Clearing House**  
An institution that electronically transmits different types of medical claims data to insurance carriers, e.g., pharmacy claims, dental claims, inpatient and outpatient claims, etc.
- » **Health Plan**  
Entity that assumes the risk of paying for medical treatments, e.g., uninsured patient, self-insured employer, payer, or Health Maintenance Organization (HMO).
- » **Healthcare Provider**  
A person trained and licensed to give health care; a place licensed to give health care, e.g., doctors, nurses, and hospitals.



Health Clearing Houses saw an **alarming 2453% year-over-year** increase in exposed records.

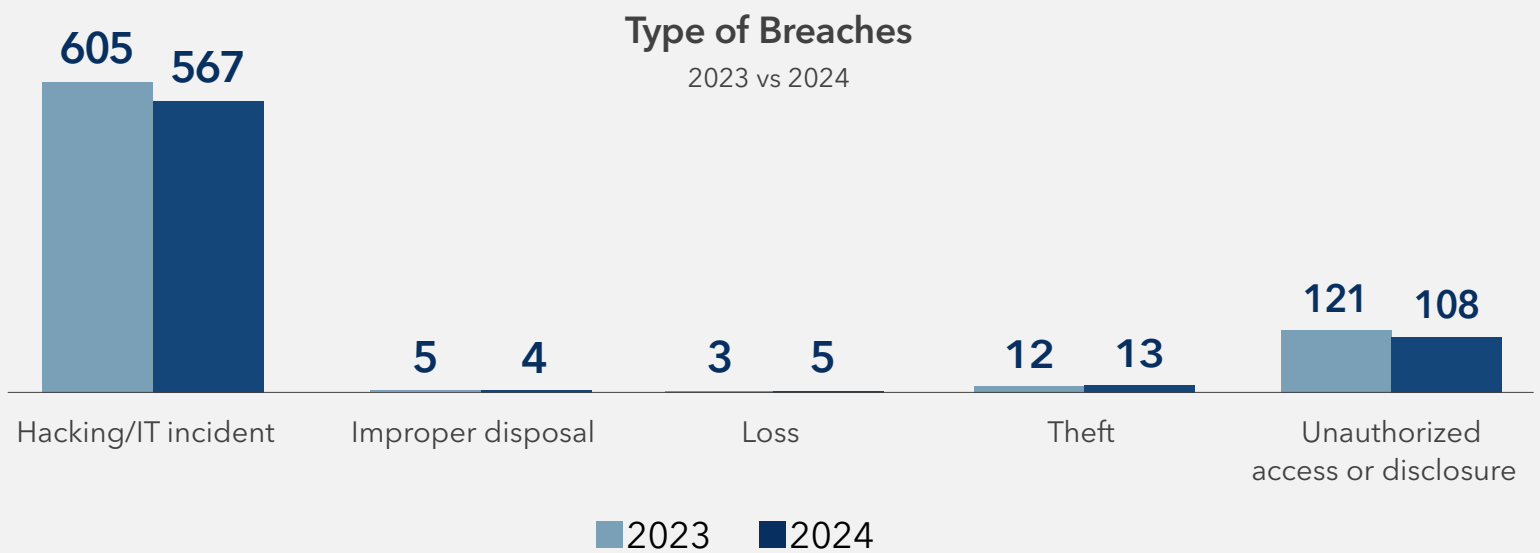
# Type of Breaches 2023 vs 2024

Hacking and IT incidents accounted for 91% of all breaches in 2024, cementing their status as the most devastating and impactful cybersecurity threat to healthcare. These attacks weren't just frequent—they were sophisticated, targeting healthcare's most critical systems with precision and intent.

Ransomware attacks led the charge, crippling organizations by locking down essential systems and demanding exorbitant payouts. Recovery costs often far exceed ransom demands, with downtime creating chaos for care

delivery, delaying treatments, and straining operations.

Malware and spyware attacks designed to siphon information over time or disrupt operations outright infiltrated network servers and endpoints. These stealthy intrusions are often undetected for months, amplifying their impact and creating cascading risks. The stakes couldn't be higher. Hacking incidents continue to dominate the threat landscape, posing risks to patient safety, operational continuity, and healthcare trust.



## Breach Type Definitions

- » **Hacking/IT Incident**  
Includes malware attacks, ransomware, phishing, spyware, or unauthorized card fraud.
- » **Improper Disposal**  
Misplaced or improperly decommissioned devices and files.
- » **Loss**  
Accidental misplacement of equipment or storage containing patient records.
- » **Theft**  
Unauthorized removal of information from a system without the owner's knowledge or authorization.
- » **Unauthorized Access/Disclosure**  
When a patient's Protected Health Information (PHI) is accessed by a third party without legal authority.

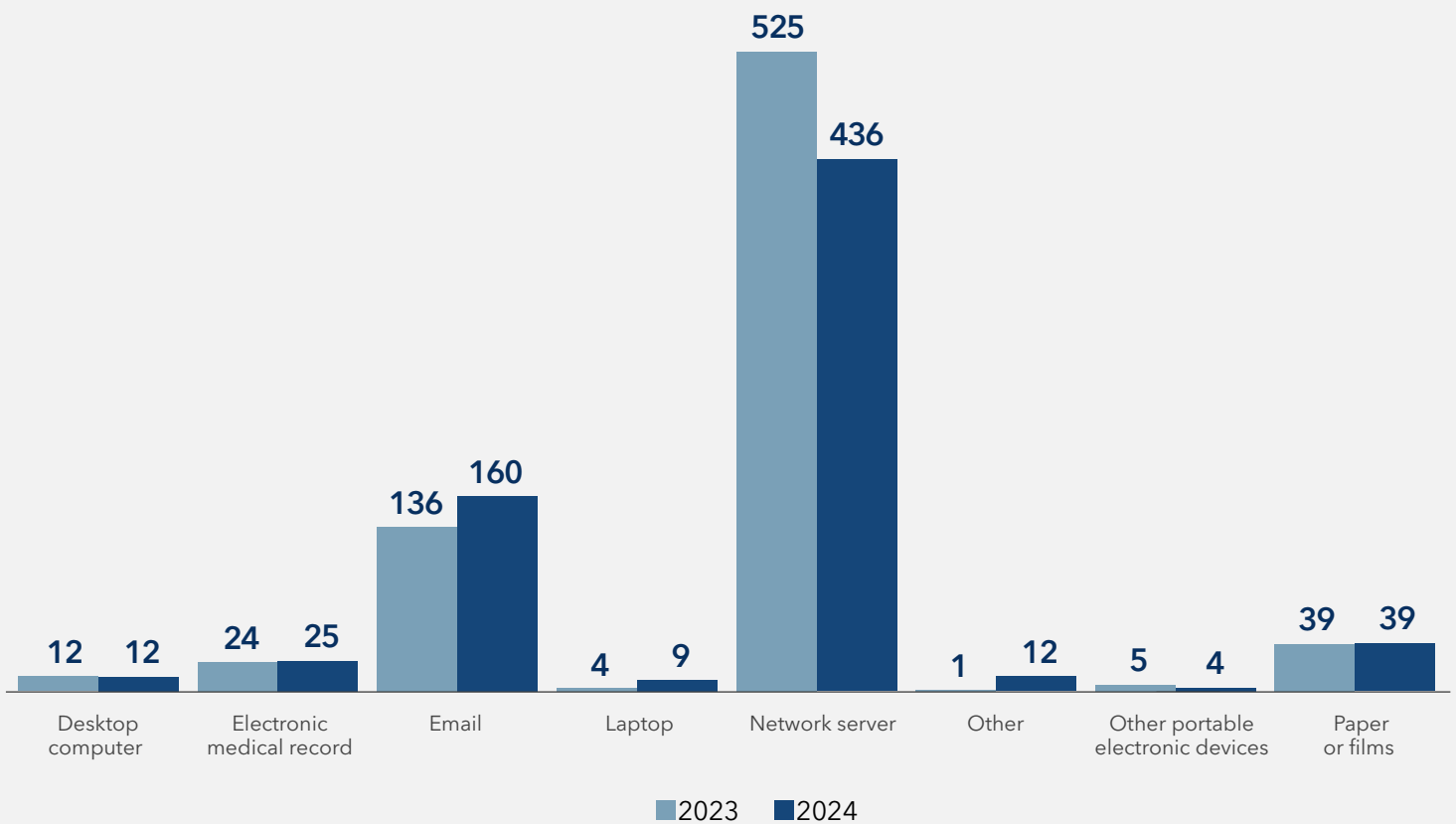
# Where Patient Data Resided When it was Compromised

In 2024, attackers leaned into familiar vulnerabilities while testing new threat vectors. Email breaches rose by 18%, reinforcing phishing as a go-to tactic.

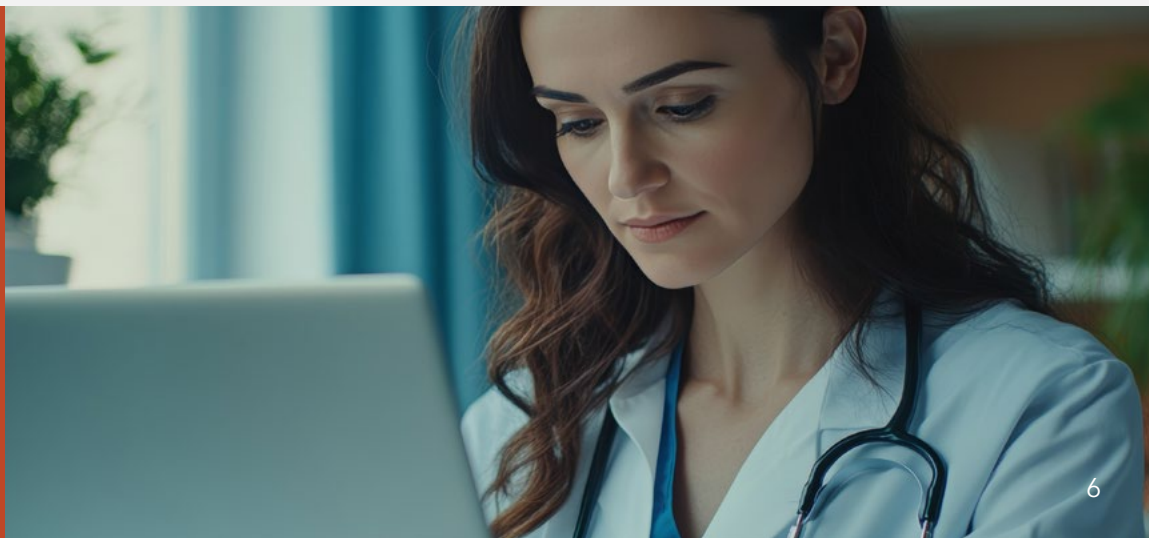
Laptops aren't just tools; they're targets. 2024 saw a 125% spike in breaches, highlighting the risks tied to portable devices in modern healthcare. Stronger encryption and better endpoint management can turn this weak link into a line of defense.

## Location of Breach Information

2023 vs 2024



**125%**  
spike in  
laptop  
breaches  
in 2024





## Addressing Threats Across the Healthcare Ecosystem

The 2024 data reveals a dual challenge for healthcare organizations: managing third-party risks and addressing vulnerabilities within their walls. Business Associates remain a significant source of breaches, while Health Plans and Clearing Houses underscore the risks inherent in interconnected systems. These third-party dependencies amplify the need for robust vendor management, compliance oversight, and collaborative risk mitigation strategies.

With breaches rising significantly in 2024, healthcare providers' email and portable devices have emerged as critical weak points. Phishing attacks and poor endpoint security remind us that even

familiar tools can become liabilities without adequate safeguards. These internal vulnerabilities demand focused efforts to strengthen defenses, train staff, and adopt advanced security measures.

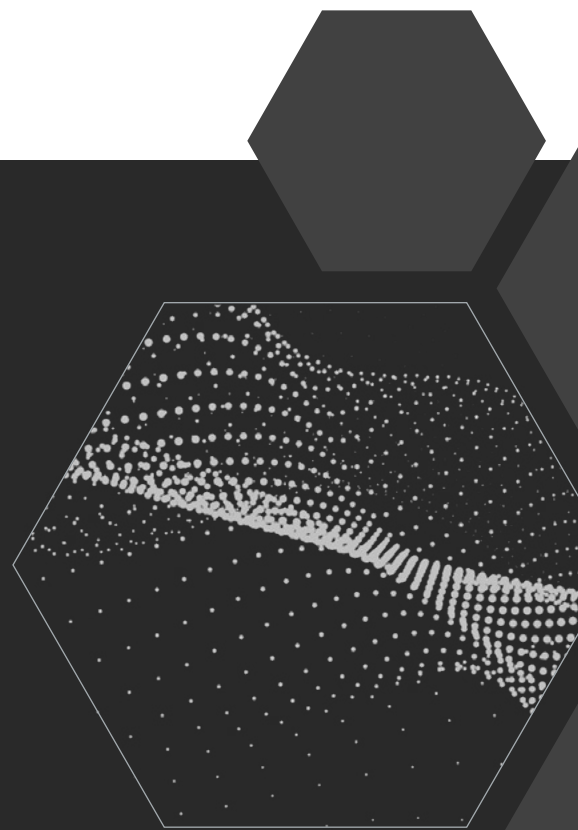
Protecting patient data in 2025 requires a holistic approach that **addresses internal risks and third-party threats.**

It all starts with empowering healthcare leaders to build a resilient, secure future for their organizations and patients.

### About this Data

This report is based on data collected from OCR's databases and public records, covering the periods from January 1, 2023, to December 31, 2024. We have undertaken efforts to scrub and clean the data to remove duplicates, ensuring higher accuracy and reliability. While we strive to maintain the integrity and accuracy of this data, please be aware that data content and accuracy may change over time due to periodic updates and additions by the OCR. Fortified disclaims any liability for errors or omissions in this data.

For further details or questions, please contact our team at [connect@fortifiedhealthsecurity.com](mailto:connect@fortifiedhealthsecurity.com).





2025 Horizon Report | 03

## Prioritizing Healthcare Cybersecurity on a Tight Budget

Healthcare organizations face a critical challenge: securing patient data while navigating tight budgets and a growing cybersecurity workforce shortage. With the looming cybersecurity workforce shortage expected to reach 85 million professionals globally in the next five years, healthcare systems are under increasing pressure to maintain strong defenses with limited resources.

In 2024, healthcare data breaches affected [over 165 million individuals](#), highlighting the urgent need for stronger cybersecurity. Tight budgets make it harder to address these challenges, especially as new technologies like IoT devices and AI platforms increase security risks. Despite these constraints, healthcare organizations can still prioritize cybersecurity and reduce risk while maximizing value.

## Understanding the Issues

Before diving into the how, it's essential to understand the why. Let's examine the four key challenges preventing healthcare from closing the cybersecurity gap: talent shortage, budget constraints, rising breach costs, and rapidly evolving technologies.

### The Cybersecurity Talent Shortage

The cybersecurity talent shortage is a critical issue across industries, but in healthcare it's also about a pronounced skills gap. According to a recent HIMSS survey, [74%](#) of healthcare organizations struggle to hire qualified security analysts, highlighting the dire need for specialized expertise.

Healthcare cybersecurity demands a unique combination of skills: master general cybersecurity principles and have deep knowledge of healthcare-specific systems like Electronic Health Records (EHRs), Internet of Medical Things (IoMT) devices, and telehealth platforms. This rare dual expertise is essential for protecting patient data and securing complex healthcare environments, yet it remains challenging to find, leaving many organizations vulnerable.

Without qualified personnel, healthcare organizations struggle to implement and maintain the security measures necessary to protect patient safety and data. Cyberattacks can lead to operational disruptions, delayed treatments, and even life-threatening situations. Additionally, non-compliance with regulations like HIPAA due to inadequate security staffing exposes organizations to hefty fines and reputational damage. Bridging this talent gap is essential for healthcare organizations to safeguard operations, maintain regulatory compliance, and protect patient lives.

### Budget Constraints in Healthcare

The growing demand for qualified cybersecurity talent drives up costs, putting even more strain on healthcare organizations already operating within tight budgets. Traditionally, these organizations have allocated only [6% or less](#) of their IT budgets to cybersecurity—significantly lower than the 10-15% spent by industries like finance and technology.

In healthcare, financial priorities often lean toward immediate needs such as patient care, medical staff, and critical equipment. For instance, a hospital may prioritize purchasing a new MRI machine over upgrading its network security. While this focus addresses short-term demands, healthcare systems are underfunded and highly vulnerable to cyber-attacks.

### The Rising Cost of Data Breaches

Despite IT's critical role in modern healthcare, this limited funding leaves significant security gaps, even as healthcare data breaches remain the most expensive, averaging \$9.77 million per incident in 2024.

The average cost of a data breach in healthcare is higher than in other industries, reaching

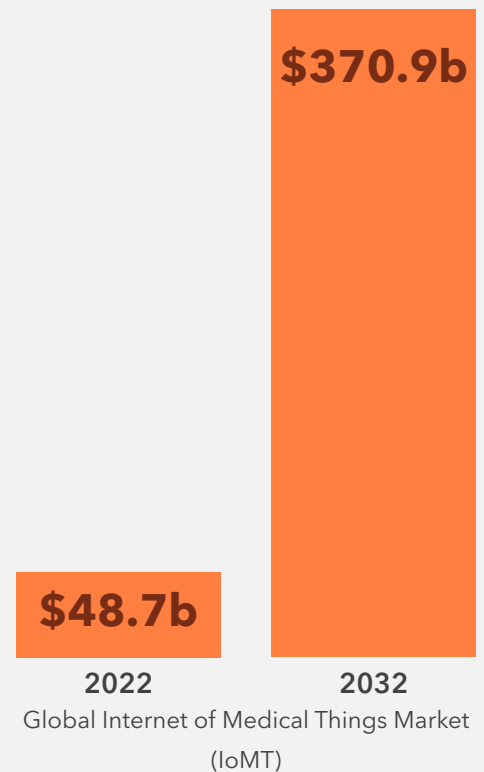
**\$9.77 million**  
per breach in 2024

Cyberattacks directly affect patient care, creating delays in medical procedures and tests. Physician care slows, and hospitals redirect patients, potentially [delaying treatment and risking lives](#). Prioritizing cybersecurity is about ensuring continuous quality care for patients while also protecting the organization's operational reputation.

## Evolving Technology and its Security Implications

As healthcare organizations adopt rapidly evolving technologies—such as EHRs, IoMT devices, and AI-driven tools—the need for regular security updates and maintenance increases. These investments are crucial for improving patient care, expanding the attack surface, and creating new cybersecurity challenges.

Projections show the IoMT market growing [from \\$48.7 billion in 2022 to \\$370.9 billion](#) by 2032, driving further demand for secure systems. However, with tight budgets, healthcare organizations must carefully prioritize these investments. Balancing the need for cutting-edge technology with the imperative to secure patient data requires smart, cost-effective strategies that maximize value while mitigating risk.



## Prioritizing Cybersecurity Risk

Organizations should conduct comprehensive [risk assessments](#) to identify critical assets and vulnerabilities and then assign resources to high-level risks. Not every element of your IT infrastructure requires the same level of security.

Focus on high-impact, low-cost cybersecurity solutions, embracing initiatives that offer the highest ROI. For instance, multifactor authentication (MFA) and phishing awareness reduce risk without significant investment.

Healthcare cybersecurity priorities should also emphasize medical device security since this directly affects patient care. [Vulnerability management for IoMT](#) mitigates device security risks.

Organizations also experience data breaches through third-party vendors.

[Third-party risk management programs](#) rank vendors, allowing organizations to focus on their highest ranked vendors driving mitigation activities to reduce risk”.

Healthcare can also mitigate risk by aligning cybersecurity investments with regulatory compliance. They can protect patients, data, and devices while meeting HIPAA/HITRUST regulations, provide more value, and avoid fines and penalties.

**Cybersecurity investments don't have to be - and shouldn't be - "one and done."**

Cybersecurity investments don't have to be—and shouldn't be—"one and done." Organizations can first mitigate critical risks and phase in other investments over time.

## Maximizing value

Hospitals must identify cost-effective solutions along with areas where cutting costs is dangerous. Patient safety and data protection must come first; these are non-negotiable areas where cutting costs can lead to severe consequences.

### Steps to Maximize your Cybersecurity Investment

#### 1. Train and Educate Staff

Invest in HIPAA regulations training to ensure compliance and protect patient health information (PHI). Regular audits and ongoing staff education reduce human error, a leading cause of data breaches. A well-trained security team serves as a human firewall, preventing costly cyber incidents.

#### 2. Strengthen Data Protection

Layer encryption and access controls to safeguard patient data from unauthorized access. These measures protect sensitive information and minimize the impact of potential breaches.

#### 3. Consolidate Security Tools and Vendors

Many organizations rely on multiple security vendors, leading to inefficiencies and high costs. Conduct regular assessments of vendor tools and contracts to identify redundancies and improve cost-effectiveness. Consolidation efforts can reduce expenses while maintaining or improving your security posture.

#### 4. Secure Cloud Configurations

Improperly configured cloud solutions are a common source of security risks. Implement cloud security posture management to ensure compliance and protect cloud environments from threats.

#### 5. Leverage Cyber Insurance

Cyber insurance provides a financial safety net for managing the aftermath of cyber incidents. However, insurers require proof of robust security practices, such as deploying and operationalizing Extended Detection and Response (EDR) tools. Meeting these requirements ensures coverage and reduces financial risk.



## Justifying Cybersecurity ROI

Organizations can demonstrate the value of cyber investments in patient safety, compliance, and outcomes. HIPAA violations can lead to fines of up to [\\$1.5 million per year](#) for each violation category. Robust cybersecurity maintains compliance. An effective cybersecurity program costs less than fines from a single major HIPAA breach.

Let's use this healthcare ROI formula. [ROI = Financial gains / Improvement investment costs](#). A \$100,000 cybersecurity investment can prevent up to \$300,000 in breach-related costs—

offering a 3x return on investment. Data Loss Prevention ([DLP](#)) solutions are an example of a low-cost investment that pays for itself many times over.

Organizations should also consider strengthening their cybersecurity posture to reduce cyber insurance premiums. If a robust cybersecurity program reduces insurance premiums by 15%, which is feasible, on a \$1 million annual premium, that's \$150,000 in direct savings.



### Value of Cyber Investments

**\$300,000** / **\$100,000**  
saved in breach-related costs      cybersecurity investment

**ROI = \$3 in value for every \$1 invested**

## Collaborative Approaches to Strengthening Cybersecurity

In the face of a cybersecurity talent shortage and tight budgets, healthcare organizations can enhance their security posture through strategic partnerships. Collaborating with entities like H-ISAC, universities, and healthcare-specific MSSPs helps share resources, expertise, and threat intelligence.

### H-ISAC

This global, member-driven nonprofit allows organizations to share cyber threat intelligence, collaborate on best practices, and reduce costs through shared resources.

## HHS 405(d) Program

Partnering with this public-private initiative provides access to free, healthcare-specific cybersecurity resources that enhance security without exceeding budget.

## University Partnerships

Collaborations with universities help create training programs and internship opportunities, addressing the cybersecurity skills gap.

## Vendor Collaborations

Working with technology vendors to develop customized security solutions ensures core clinical systems are protected without the need for extensive in-house expertise.

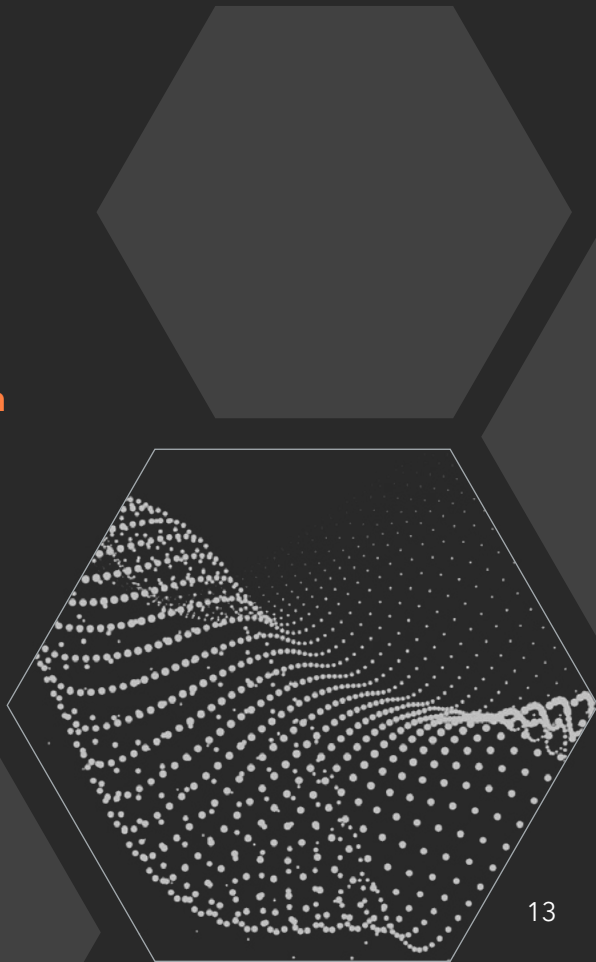
## Healthcare-specific MSSPs:

Outsourcing to MSSPs provides 24/7 monitoring, threat intelligence, and incident response, offering enterprise-grade security at a fraction of the cost of an in-house team.



## Building a Resilient and Cost-Effective Cybersecurity Strategy

Securing the future of healthcare requires prioritizing cybersecurity to protect patient care and data. **By making smart investments in talent, technology, and strategic partnerships, healthcare organizations can strengthen their security posture without exceeding budget constraints.** A clear ROI justifies each investment, ensuring that cybersecurity is not only an expense but a crucial component of patient care and regulatory compliance.





2025 Horizon Report | 04



Guest Author  
**Paul Connelly**

# Communicating with Your Board: Telling Your Story and Using Metrics That Matter

Three major disrupters have been pushing cybersecurity and technology risk up the priority list for boards of directors at healthcare organizations:

## 01

Cybersecurity threats to patient care and business operations, and their potential for significant financial, regulatory, and patient trust impacts.

## 02

The need to balance trust with the urgency to utilize AI and other technologies to drive innovation, quality, and efficiency.

## 03

Regulatory and stakeholder expectations for boards to actively oversee the management of cybersecurity and technology risks.

As a result, cybersecurity leaders are gaining greater access to their board. Being able to successfully engage to articulate risks, the strategy of their program, and the value it delivers can help a security leader build long term success.



# Up Your Game to Make the Most of this Opportunity

This focus by the board is a tremendous opportunity to build understanding and support at the top. Taking full advantage requires developing the right message, supporting it with the right data, and presenting in the right way.

## 01 The Right Message - Tell the Story and Start a Conversation

A board wants to know four broad things -

- » **What are our biggest risks?**
- » **Is our program doing the right things to manage them?**
- » **How well are we doing?**
- » **What obstacles are in the way?**

Those are not yes or no questions, and a security leader can stimulate informative discussion by telling the story of their program. Keep the slides to a minimum and aim for a discussion on the factors that cause risk, how the program protects and enables business strategy, and the challenges faced.

Approach the discussion like a business plan and speak in terms of -

- » **Strengths:** Progress being made and the return on investments
- » **Weaknesses:** Risks that need attention and obstacles to success
- » **Opportunities:** Proposed actions that will reduce business impacts
- » **Threats:** Changes in threats, regulations, legal risk, and other potential impacts on business objectives like revenue growth, market share, and customer satisfaction

Focus on bringing solutions, not just problems. Cybersecurity is a big risk in healthcare, and your board knows that, so it is important to have an action plan or strategy for every risk raised.

## 02 Supporting your Message with the Right Data - Climb the Pyramid

Metrics add credibility to your story when used properly. They can show the effectiveness of the program by measuring coverage, speed, and accuracy. They can highlight efficiencies gained through automation, innovation, and productivity. Most importantly, metrics can support the story of reducing risk, preventing events, and returning value from investments. Unfortunately, metrics can also be a distraction, confusing, and overwhelming to a board, so it is important not to let them *become the story*.

Think of metrics like a pyramid. The dashboard a security leader uses to run and monitor day-to-day operations is the base - wide with deep details and measures. The messages and data used in discussions with business leaders are the middle - less detail and more combining of metrics to highlight operations and business impacts. What goes to the board should be the peak - less data and rolled up summaries that point to a story.

For example, cybersecurity SOC tools can produce metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), True Positives/False Positives, and the total number of security incidents detected. Those are important for running the security program but are not the right level for a board meeting. A summary of "Threat Detection & Response Capabilities" that is based on a roll-up of those metrics would be more relevant. Similar rolled-up measures can tell the story of other key risks such as third-party risk management, compliance, and cloud security posture.

One last note on metrics - be certain you can explain and prove the accuracy of anything you present to the board, and why it is relevant. A good rule of thumb for gauging relevancy is to ask, "what does it mean if this measure changes?" - if it doesn't drive a response, it is likely not needed.

### 03 Presenting in the Right Way

The chairman of the audit committee at my last company used to always ask me, "What is keeping you awake at night?" at the end of my quarterly updates. I realized the genius in that question was to give me a chance to break from PowerPoint slides to an open discussion. While meeting times with a board tend to be tightly scheduled, engaging in discussion makes for an effective meeting. Some practices to facilitate discussion include:

» **Know your audience**

Your board has a fiduciary responsibility to stakeholders to ensure management is taking appropriate, legal, and ethical action to address risks. Their role is oversight - which is not the same as management. Your board is likely a group of highly accomplished healthcare and business leaders, but with limited expertise in cybersecurity and technology.



**Be proactive**  
about getting  
information to  
your board.



» **Speak their language**

The role and makeup of your board warrants a different level of technical detail than an internal presentation to business leaders. Your language needs to be high level and concise, and you must be careful not to overwhelm them with data, jargon, or acronyms.

» **Choose the right tone**

Be transparent and don't sugarcoat your message but approach it as a business problem - not with scare tactics. The board needs to know about incidents, progress, and gaps; but discuss them in terms of business impacts and propose solutions.

» **Provide context**

Mapping your program to recognized standards such as the NIST CSF, providing examples from others in your industry, and including feedback from independent partners help your board understand how your program is doing.

## **Additional Ideas - Be Proactive**

A strong board wants to understand the risks and how they are being addressed, so use every lever available to build their awareness.

- » Can you provide a separate cybersecurity awareness briefing?
- » Involve the board in a tabletop exercise?
- » If you plan to talk about ransomware defenses in your update, can you put a one-page overview of how ransomware attacks work in the pre-reading material for the board meeting?

Be proactive about getting information to your board.

Line up allies like the CIO, your Internal Audit leader, and Legal Counsel and pre-brief them on your message and metrics to rehearse your presentation, get feedback, and anticipate questions. Ask them to play the role of harsh critics to get issues on the table before the board meeting.

Remember, it is not limited to a once-a-quarter interaction at the board meeting. Clear it with your CEO, but the discussion can continue between board meetings with follow-ups on questions, sharing news relating to discussions, or awareness materials.

**By making the most of interactions with the board, cybersecurity leaders can develop their role as business leaders and position their program for long term success.**



2025 Horizon Report | 05

# The Future of Healthcare Cybersecurity Legislation: **A Collective Push Toward Resilience**

More than a year ago, the Department of Health and Human Services (HHS) announced its intention to update the HIPAA Security Rule to better protect our healthcare infrastructure against a growing wave of cyberattacks. Yet, in the months since, healthcare providers, plans, and their partners have been hit with 472 breaches, underscoring both the urgency to act and just how interconnected we truly are. Any attack – even one at a small, rural hospital – has the potential to impact the entire ecosystem, threatening the stability of larger networks and putting providers, patients, and communities at risk.

In response, various legislative proposals have emerged with New York taking the boldest step by enacting its own stringent cybersecurity rules in a move that is likely to inspire other states to follow suit – especially if federal efforts remain stalled.

As additional states consider similar mandates, healthcare providers may soon find themselves navigating a complex landscape of overlapping federal and state requirements. Certainly, this could result in stronger sector-wide defenses, but it could also create challenges for consistent compliance across jurisdictions.

# Setting the Bar for Healthcare Cybersecurity

In December 2023, HHS introduced a strategic framework for guiding cybersecurity improvements across healthcare through four key initiatives which outline the foundation of essential and enhanced cybersecurity goals across the sector. These proposed changes also include updates to the HIPAA Security Rule, which is long overdue with the last updates over twenty years ago.

## Establish voluntary cyber performance goals

Originally intended as best practices, these goals are likely to become benchmarks that all healthcare providers must meet.

## Provide incentives and funding

Recognizing the unique challenges faced by smaller, under-resourced providers, the framework includes federal funding to help these organizations implement essential protections.

## Make standards enforceable

The updated HIPAA Security Rule is likely to incorporate both essential and enhanced cybersecurity goals, requiring compliance from any organization handling protected health information (PHI).

## Harmonize the government's approach

To streamline compliance, HHS aims to coordinate cybersecurity standards across federal agencies, creating a unified approach to strengthening defenses across the sector.

Perhaps most notably for healthcare providers, non-compliance could carry severe financial consequences, such as increased Office for Civil Rights (OCR) fines and potential Centers for Medicare and Medicaid Services (CMS) funding reductions for hospitals.



Any attack – even one at a small, rural hospital – has the potential to **impact the entire ecosystem.**

# Bipartisan Legislative Efforts to Address Healthcare Cybersecurity

Three bipartisan legislative proposals were introduced in 2024, highlighting the urgency among policymakers to establish more rigorous standards, enhance accountability, and mitigate the growing cyber threats facing our nation's healthcare systems.

## Healthcare Cybersecurity and Resiliency Act of 2024

Introduced in November 2024 by Senator Cassidy (R-LA), along with Senators Warner (D-VA), Cornyn (R-TX), and Hassan (D-NH), this legislation focuses on improving the overall cybersecurity posture of healthcare and public health sectors through collaboration between the Department of Health and Human Services (HHS) and the Cybersecurity and Infrastructure Security Agency (CISA). It emphasizes the creation of a comprehensive cybersecurity incident response plan, offers grants for public or non-profit healthcare providers, and updates existing regulations to create cybersecurity standards. It also includes provisions for sharing threat information, enhancing training, and strengthening infrastructure. With Senator Cassidy currently serving as the ranking member of the HELP committee, and soon to become the Chair of that committee, we are hopeful that this bi-partisan legislation will pass early in the coming year.

## Healthcare Cybersecurity Act of 2024

Introduced in the Senate, then similarly in the House, the Healthcare Cybersecurity Act aligns with the Biden administration's 2023 National Cybersecurity Strategy,

emphasizing public-private collaboration and sector-specific security improvements. Building on this foundation, the act proposes enhancing resource allocation, establishing secure channels for real-time information sharing, and strengthening support for healthcare providers. The majority of items called out in this Act are items that are already being accomplished by CISA and HHS, but this legislation would solidify the future of these programs.

## Healthcare Infrastructure Security and Accountability Act (HISAA)

Proposed in the Senate, the Health Infrastructure Security and Accountability Act would mandate annual audits of large healthcare organizations, expand penalties for non-compliance, and, notably, require CEOs and Chief Information Security Officers (CISOs) to attest to their organizations' cybersecurity compliance personally.

Additionally, the proposed bill allocates \$1.3 billion in funding for critical access hospitals starting in 2027 to support resource-limited organizations. However, with phased penalties for non-compliance by 2028, many under-resourced providers may still face funding gaps.

While these legislative initiatives are predominately bi-partisan and reflect a collective push for more robust cybersecurity measures across the healthcare sector, it remains to be seen whether they will make it out of committee given the change in administration. Most likely, if they do, it will be in a revised version of what has been proposed.

## State-Led Action: New York Sets a Precedent

While federal regulations remain stalled, New York's proactive stance points to an obvious conclusion: What once was voluntary will soon be mandatory. Effective October 2, 2024, New York's cybersecurity law requires hospitals to report cyber incidents within 72 hours and fully comply with extensive security measures within a year. Covering more than 200 hospitals, this mandate is the first of its kind in the U.S. and likely to set the stage for similar legislation at the state level.

As more states consider their own cybersecurity requirements, healthcare providers operating across state lines could face a layered mix of compliance obligations, navigating both federal and state-specific rules.

## Upcoming Cyber Incident Reporting Requirements Under CIRCIA

In July 2024, the public comment period closed for the Notice of Proposed Rulemaking (NPRM) under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). This legislation, once finalized, will establish mandatory reporting rules across all critical infrastructure, requiring organizations to report cyber incidents within 72 hours and ransom payments within 24 hours.

The Cybersecurity and Infrastructure Security Agency (CISA) is currently reviewing the feedback received and aims to issue the final rule by October 2025. This impending regulation is designed to improve national response and resilience to cybersecurity threats by standardizing reporting protocols for significant incidents.

Given the potential impact on critical infrastructure, it is crucial for organizations to stay informed and prepare for compliance. We are closely monitoring the developments related to CIRCIA and recommend that our clients do the same to ensure readiness for these new reporting obligations.





## Preparing for Compliance: A Collaborative Path Forward

As healthcare cybersecurity regulations evolve, leaders across the sector must act decisively. Building strong cybersecurity practices is no longer just about checking a box for compliance; it's essential for safeguarding the healthcare ecosystem.

To effectively prepare for evolving requirements, healthcare providers should:

### Conduct a Comprehensive Gap Analysis

Providers should begin with a thorough assessment of their current cybersecurity landscape. Identifying and prioritizing gaps enables efficient resource allocation and targeted remediation.

### Explore Available Federal Support for Resource-Limited Providers

While not all organizations may qualify, certain federal programs, including HHS's proposed 2025 budget, aim to support under-resourced hospitals in implementing and maintaining essential cybersecurity measures.

### Strengthen Vendor and Third-Party Compliance

As standards expand to cover non-PHI data, healthcare providers must ensure vendor contracts reflect updated security requirements. Regular assessments are crucial for verifying compliance, particularly as third-party vulnerabilities can become entry points for cyber threats.

Healthcare organizations without established cybersecurity programs must begin by tackling the essential goals. Meanwhile, those that already meet foundational standards would be wise to advance toward enhanced goals in anticipation of a future in which these benchmarks are the norm.



## Addressing the Unique Needs of Smaller Providers

While new legislation will challenge all organizations, small and rural healthcare providers will face the greatest challenges. Despite initiatives from companies like Google and Microsoft offering discounted or free tools, adoption remains limited due to:

### Compatibility issues

Many smaller providers rely on systems that may not integrate well with newer cybersecurity tools.

### Data privacy concerns

Organizations are cautious about how Google and Microsoft might handle their data, raising privacy and security concerns.

### Resource constraints

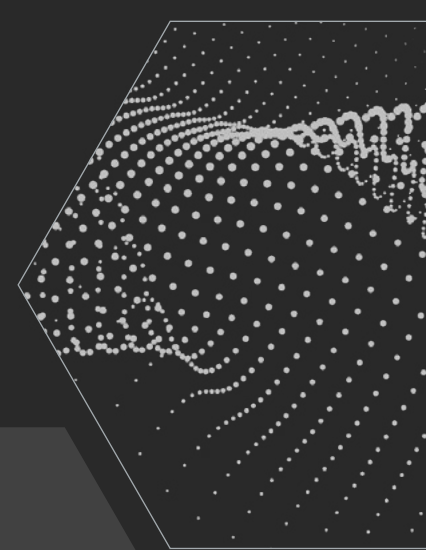
Limited budgets and a shortage of specialized cybersecurity talent prevent smaller providers from fully implementing these solutions, as well as monitoring and maintaining them.

Addressing these unique needs with adaptable, cost-effective solutions is a must – not only for their security but for the resilience of the entire healthcare system.

## Embracing a shared responsibility: Building a secure future together

**The shift toward mandatory cybersecurity standards reflects a critical, shared responsibility across the healthcare sector.** Every organization—from large, multi-state systems to small rural providers—plays a critical role in preventing cyberattacks that create patient safety issues, and long-term patient confidentiality concerns.

Building a secure healthcare ecosystem is more than compliance; it's about creating a unified system that protects patients, providers, and communities nationwide. Through public-private partnerships and real collaboration, healthcare leaders have an unprecedented opportunity to create a more secure future for everyone, but it will take all of us to make it a reality.





2025 Horizon Report | 06

# AI: A Double-edged Sword Shaping the Future of Hospitals

While AI offers unprecedented benefits to healthcare organizations, this technology is a double-edged sword.

As the healthcare ecosystem embraces the digital transformation artificial intelligence (AI) has provided - enhancing patient care, optimizing operations, and driving data-based decisions - it also creates new vulnerabilities that can endanger patient safety and disrupt hospital operations.

With the surge of Generative AI, cyber-attacks are becoming increasingly complex, forcing healthcare providers to balance finding ways to protect sensitive data and systems while innovating. But how can organizations do both? Let's look at the evolution of AI-driven cyber-attacks, explore AI's dual role as defender and disruptor, and identify the best strategies to build resilient healthcare systems with a balance of innovation and security.

## AI-Generated Cyberattacks: A New Threat to Hospitals

AI-driven cyber-attacks represent a new class of threat vectors in which adversaries leverage machine learning and artificial intelligence to execute increasingly sophisticated attacks. These include everything from data breaches and disinformation campaigns to automated bot attacks and AI-generated phishing scams.

### AI Phishing Scams

Generative AI's malicious use makes it easier for cybercriminals to create more realistic, harder-to-detect, and more specific phishing attacks.

By training AI models on large text datasets to create emails that resemble a hospital's official communication style or even the writing style of specific individuals, attackers are creating personalized messages that employees have more difficulty identifying as fraudulent.

Even the most well-trained healthcare staff can fall for these realistic phishing emails, and with hundreds or thousands of them inundating healthcare every day, it is not surprising to see the resulting stolen login credentials and compromised sensitive data.

## AI-Enhanced Targeting of Hospital Networks

According to trends we've witnessed with our customers, cybercriminals have shifted to employing AI to orchestrate complex attacks on one of their prime targets-hospitals.

AI-generated cyberattacks walk through every machine learning algorithm to find vulnerabilities within hospital networks so methods can be adjusted as needed. For instance, criminals can use AI to create ransomware that almost instantly learns how a hospital system works and intelligently shuts down its key services, making it impossible for that hospital to function without paying a ransom.

### Threat to Patient Privacy and Data Integrity

Healthcare data is among the most valuable information on the dark web, making AI-driven attacks on healthcare organizations especially harmful. Criminals can sell patient information for identity theft or manipulate records to disrupt care. The sophistication and adaptability of AI-driven attacks present a severe risk to patient privacy and data integrity, highlighting the urgent need for robust cybersecurity strategies in healthcare organizations.



Cyber-attacks are becoming **increasingly complex**, forcing healthcare providers to balance finding ways to protect sensitive data and systems while innovating.

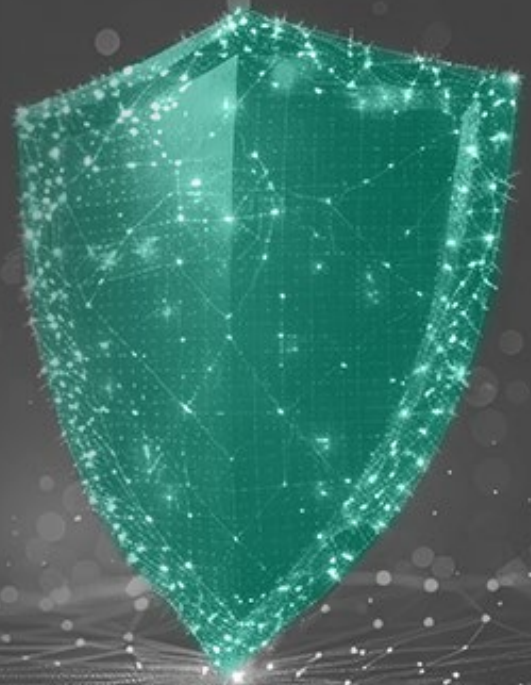
# The Rise of AI in Cybersecurity: A Tool for Both Attackers and Defenders

We appear to be on a never-ending yo-yo in healthcare cybersecurity. While AI has been used in clinical settings for decades—primarily in decision support—it now plays a dual role, serving both attackers and defenders in cybersecurity.

## Defenders

### Using AI as a Shield in Cybersecurity

For defenders, AI-powered tools are essential for identifying and responding to real-time threats. These systems can sift through mountains of data to identify abnormal behaviors that could be signs of a cyberattack, enabling the hospital cybersecurity team to take preventive action. Machine learning algorithms can even confirm vulnerabilities in a hospital network and propose ways to remain one step ahead of hackers.



## Attackers

### Leveraging AI for Adaptive Cyber Threats

Attackers are increasingly leveraging the same technologies used by their targets. Hackers are adopting adaptive AI-driven malware, predictive attack methods, and even testing defenses without human input. As both sides continuously update their strategies in response to each other, it creates a complex landscape for hospitals. To avoid risk, hospitals must invest in and stay aware of innovations in cybersecurity.

## Progress on AI Regulation: Safeguarding Healthcare Security

As AI becomes more critical to care delivery and hospital operations, regulatory bodies are becoming aware of cybersecurity's essential role in healthcare. Smart regulations on AI may even create safeguards against risks by stipulating processes for using health data, the functioning of the system, and responsibility for algorithms.

Healthcare-specific regulations, such as those from the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), and the Food and Drug Administration (FDA), focus on protecting patient data and ensuring that AI systems meet rigorous privacy

standards. More precise guidelines will support hospitals in adopting responsible AI practices. However, until then, proactive compliance measures, such as third-party audits and transparent practices, are essential for security.

Finding the right equilibrium between innovation and regulation is vital. Excessive regulation may undermine the potential benefits that AI can bring to healthcare, while insufficient regulation could expose hospitals to cyber-attacks. While awaiting clearer AI guidelines, many hospitals proactively ensure compliance through third-party audits and transparent algorithm explanations.



Finding the right equilibrium between **innovation and regulation** is vital.

## AI in Healthcare: Applications and Associated Risks

AI also plays a role in hospitals by analyzing data, predicting when beds might be available, and optimizing staff productivity overall. For example, [Elon Musk](#) suggested his new AI engine, Grok, can analyze medical images. However, such applications bring particular cybersecurity risks. Because these systems rely on large volumes of patient data, a security breach

could expose a significant amount of sensitive information. Also, if an AI system used in a diagnosis or treatment recommendation—perhaps through analyzing medical data on electronic health records—is manipulated, then it could lead to an inaccurate diagnosis or inappropriate treatment and directly affect patient care.



**Human error** remains one of the weakest links in security defenses.



So, while the potential for diagnostics and health care is indeed fascinating, the risks are still being better understood.

From what we know today, addressing these risks demands a holistic approach:

### **Encrypting Data and Controlling Access**

Hospitals encrypt all patient information, making it only accessible to employees within the facility who are authorized to have it. Enhanced security measures, like two-step verification and restricted entry to specific AI programs, prevent the leakage of classified documents.

### **Ongoing Monitoring**

With a trusted partner like Fortified, healthcare providers receive expert-driven, continuous monitoring, ensuring they have the guidance and support needed to stay secure. Meanwhile, AI-driven monitoring systems complement these efforts by detecting real-time anomalies and alerting providers to unusual activity before it can escalate into a breach. Hospitals need comprehensive monitoring solutions that combine the expertise of a trusted partner with the power of advanced technology to identify and address emerging threats in real-time.

### **Regular Security Audits**

Audits, including “adversarial testing,” would identify and fix vulnerabilities in AI systems. While hospitals may not be able to launch a full-fledged red teaming effort, they can try penetration testing to get a feel for what type of attack their networks might see.

### **Regularly Train Staff on Cyber Hygiene**

Human error remains one of the weakest links in security defenses, and hospital staff should be trained on cybersecurity dos and don’ts to reduce mistakes. Training staff in phishing strategies, methods of handling data securely, and password security can mitigate some risks.

### **Cooperation and Knowledge Exchange**

Hospitals will benefit from the knowledge of other health organizations, security companies, and government partners, so cooperation with others is a must in managing AI and general cybersecurity risks.



## The Path Forward: Building a Resilient Healthcare Cybersecurity Ecosystem

**AI is transforming healthcare, offering huge potential for improving patient care and operations, but it also brings significant cybersecurity risks.**

Healthcare organizations must adopt proactive and adaptable cybersecurity strategies to protect sensitive data and ensure patient safety. As AI technology continues to evolve, healthcare providers need to balance innovation with security, stay aware of emerging threats, and collaborate with regulatory bodies. By doing so, they can safely harness the power of AI while safeguarding their systems and fulfilling their mission of patient care.



# Threat Actor Evolution in Healthcare Cybersecurity

Today's attackers are more persistent and calculated than yesterday. They now employ an array of advanced tactics that demand a strategic and resilient cybersecurity posture from healthcare institutions. The anatomy of threat actor attacks in healthcare has become a sophisticated, multi-pronged threat, exploiting vulnerabilities across healthcare systems and data infrastructures.

So, how can healthcare organizations protect their data from these evolving threats? You must understand them. That understanding starts here with three trends: the escalation of ransomware tactics, repeat attacks, and mega breaches.



## Ransomware 2.0: Double Extortion and Data Theft

Cybersecurity threats have evolved far beyond traditional ransomware. Known as “Ransomware 2.0,” double extortion tactics are now the norm. Attackers now not only encrypt the data but also steal it and threaten public release if the ransom is not paid. This raises the stakes, particularly for healthcare organizations, where patient confidentiality and regulatory compliance are crucial.



Today’s attackers are more **persistent and calculated**, employing an array of advanced tactics that demand a strategic and resilient cybersecurity posture from healthcare institutions.

## Repeat Attacks on Healthcare Systems

Once doesn’t seem to be enough anymore for threat actors. Now they are increasing repeat attacks on healthcare systems, that are even more sophisticated than the first.

For example, the 2023 & 2024 attacks on [McLaren Health Care](#) led to significant operational disruptions, with some patient services affected for weeks.

## Why Repeat Attacks are Increasing

### Inadequate remediation

After an attack, healthcare providers may focus on restoring essential services, sometimes leaving longer-term security issues unaddressed. Attackers exploit these “post-attack gaps,” which might remain open while hospitals scramble to resume patient care.

### Cyber fatigue

Health systems often face “cyber fatigue,” where security teams are overwhelmed, making them more vulnerable to additional attacks. Even after an initial attack, healthcare organizations may struggle with follow-up defenses, especially if resources are stretched thin.

### Revenue impacts

Cyber attacks are well known to affect the revenue operations of a facility. That impact is felt across the organization, including the security and IT departments. A loss in revenue makes needed investments exceedingly challenging.



Attackers now not only encrypt the data but also steal it and **threaten public release** if the ransom is not paid.

## Mega Breaches: Analyzing the Scale and Scope

The scale and frequency of attacks have created a wave of mega breaches across the healthcare ecosystem, impacting millions of patients and generating significant regulatory and reputational fallout. With sensitive patient data and essential services at risk, healthcare cybersecurity leaders are under increasing pressure to respond effectively.

Recent examples include the [Change Healthcare breach](#), the largest ever reported in the United States, which exposed 100 million patient records. This breach underlined the vulnerability of large data repositories and the widespread impact of these breaches.

## Strategic Imperatives for Healthcare Leaders

To counter this, healthcare Chief Information Security Officers (CISOs) and IT leaders must prioritize creating a layered security strategy that goes beyond playing defense.

Healthcare systems need to create an integrated approach that includes:

- » Encompassing enhanced monitoring
- » Robust incident response plans
- » Continual testing of security measures

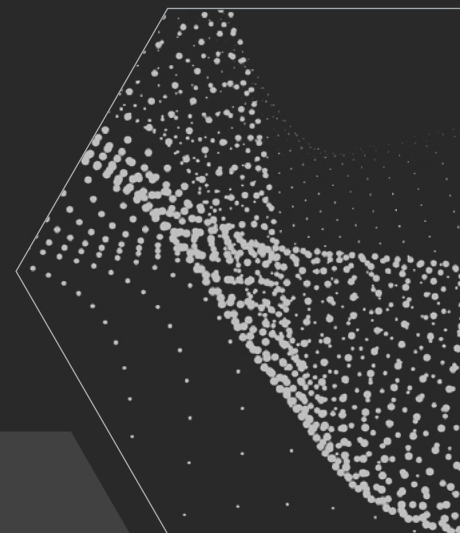
Securing patient data and maintaining uninterrupted access to critical care services are paramount; there is no room for error. As a result, healthcare institutions are deploying layered security solutions that encompass preventive, detective, and corrective measures. These include advanced threat detection systems, network segmentation, frequent security assessments, and incident response simulations.

This layered, resilient security posture allows healthcare systems to stay one step ahead of sophisticated cyber threats. Do not misunderstand; these potential threats will never be eliminated, but a proactive, integrated approach to cybersecurity significantly reduces the risk and impact.



## Looking Forward

As healthcare cybersecurity continues to face intensified attacks from threat actors, **healthcare organizations must strategically focus on resilience and proactive defense to face these evolving challenges.** By building a layered approach, healthcare communities can build a stronger line of defense to better defend against sophisticated attacks. Embracing these principles will be crucial in adapting to a rapidly changing digital threat landscape and securing the future of healthcare.





2025 Horizon Report | 08

# Advancing Third-Party Risk Management in Healthcare

Healthcare systems today are under constant pressure to protect patient data and maintain operations amid growing cyber threats. For leaders in healthcare, managing third-party relationships is key to ensuring security and resilience—yet these partnerships also bring significant risks.

Effective Third-Party Risk Management (TPRM) is key to identifying, assessing, and mitigating these risks. However, TPRM maturity varies widely across the industry. For healthcare leaders, advancing through TPRM maturity stages is essential to building a comprehensive risk management framework that protects patient trust, supports operational continuity, and strengthens organizational security.

# Key Examples Highlighting Third-Party Management Challenges

Recent high-profile incidents underscore the significant risks healthcare organizations face due to third-party vulnerabilities:

## OneBlood Ransomware Attack

July 2024

OneBlood, a major supplier of blood and blood products serving over 350 hospitals, experienced [a ransomware attack](#) that severely disrupted its blood delivery operations. This breach highlights the impact third-party disruptions can have on healthcare services, as well as the critical need to include essential suppliers in a comprehensive TPRM program

## Change Healthcare Data Breach

February 2024

Change Healthcare, a leading provider of services and solutions to healthcare organizations was targeted in the most significant HIPAA-regulated data breach involving protected health information (PHI). The ransomware attack compromised PHI for at least 100 million individuals, demonstrating the substantial risks posed when third-party vendors handle large volumes of sensitive data.

## Third-Party Risk Management Incremental Maturity

These cases demonstrate the critical need for a mature TPRM program to help proactively identify, evaluate, and mitigate third-party risks, ensuring operational continuity and safeguarding patient information.

Below are the five levels of TPRM maturity. Knowing your organization's current level can help guide the targeted actions you should take to improve its security and resilience.



### Limited or Unreliable Inventory of Third-Party Suppliers

At the most basic level, many organizations lack a comprehensive and reliable inventory of their third-party suppliers. While critical partners, such as those providing EHR systems, patient accounting, or imaging services, may be informally identified, there is often no systematic record-keeping. Without a reliable inventory, effectively monitoring and managing associated risks is difficult.

#### **Action Plan**

#### **Conduct a comprehensive Business Impact Analysis (BIA).**

Organizations at this stage should start by creating an accurate inventory of third-party suppliers and then conducting a BIA. A BIA identifies the most critical suppliers and assesses potential disruption impacts, setting the groundwork for progression to the next level.



## 02

### Identifying Critical Suppliers Without Risk Insight

At this maturity stage, organizations begin identifying critical third-party suppliers but do not completely understand the risks these suppliers pose to operational resilience.

#### **Action Plan**

**Integrate critical suppliers into the risk management program.**

Organizations must move beyond merely identifying critical suppliers and begin integrating them into a structured risk management process. This process includes obtaining independent audit reports and reviewing control environments to establish a baseline for risk.

## 03

### Inconsistent Pre-Purchase Assessments

Third-party assessments are performed inconsistently at this stage, happening before a purchase. Organizations often start by creating a questionnaire, typically in a spreadsheet format, for vendors to complete. While this approach provides a useful snapshot of specific aspects of the vendor's solution, it offers only limited insight into potential risks.

#### **Action Plan**

**Formalize the integration of critical suppliers into a standardized risk management process.**

Organizations at this level should formalize and standardize TPRM assessments as a consistent onboarding step for new vendors.

## 04

### Integrated Procurement and TPRM Processes

A significant maturity leap occurs when organizations integrate TPRM assessments directly into their procurement processes. At this level, risk assessments are required before purchasing new solutions, ensuring that potential risks are identified and considered early in the decision-making process. This approach reduces the chance of onboarding high-risk vendors. Integration with procurement also fosters collaboration between departments and promotes a proactive risk management culture.

#### Action Plan

**Identify alternative suppliers to minimize disruptions.**

Organizations should start identifying alternative suppliers to strengthen operational resilience and minimize the impact of single points of failure.

## 05

### Comprehensive and Mature TPRM

At the highest level of maturity, organizations have established a consistent and comprehensive TPRM program. This program goes beyond assessing new solutions to include periodic evaluations of existing third-party relationships. Continuous monitoring and risk acceptance processes are in place to support ongoing vendor risk management. A mature TPRM program sustains operational resilience by effectively managing third-party risks across all stages of the vendor lifecycle.

#### Action Plan

**Leverage multiple suppliers and continuous monitoring.**

Organizations at this level should regularly reassess vendors, incorporate a risk acceptance process, and maintain a robust strategy to address potential vendor disruptions and ensure operational stability.

## Level up your TPRM program

**A mature TPRM program is essential to safeguard patient care and strengthen resilience against rising cyber threats.**

By advancing your TPRM maturity level and following the action steps outlined above, your organization can take a crucial step toward lasting security and operational stability.



2025 Horizon Report | 09

# Cybersecurity Outlook for 2025: Key Insights for the Year Ahead



# On the Horizon

## Increased Outsourcing of Healthcare Cybersecurity

By 2025, healthcare organizations will increasingly rely on managed security service providers (MSSPs) and specialized third-party vendors for cybersecurity. This strategy will help mitigate critical talent shortages, ease the burden on internal teams, and ensure access to advanced expertise and technology, enabling organizations to stay ahead of the rapidly evolving threat landscape.

## Adoption of Zero Trust Architectures

By 2025, healthcare organizations will begin embracing the principles of Zero Trust Architecture (ZTA), but full implementation will remain a long-term goal. Most will focus on foundational steps like network segmentation, multi-factor authentication (MFA), and identity management to build toward Zero Trust. These incremental changes will enhance security while accommodating the constraints of legacy systems, resource limitations, and compliance requirements. This phased approach reflects a practical shift toward Zero Trust adoption, driven by regulatory guidance and the need to address evolving cyber threats.

## Challenges for Prioritized Security for Internet of Medical Things (IoMT)

In 2025, securing Internet of Medical Things (IoMT) devices will continue to pose significant challenges for healthcare organizations, with persistent vulnerabilities highlighted by a 2024 report from Forescout Research identifying medication dispensing systems as particularly exposed. Despite these challenges, healthcare organizations are increasingly prioritizing cybersecurity. A survey conducted between August and September 2024 revealed that 60% of health system executives plan to focus on improving cybersecurity in 2025.

However, the complexity of IoMT security, coupled with limited resources and competing priorities, means that comprehensive solutions may be slow to implement. As a result, while awareness and concern about IoMT vulnerabilities are rising, the pace of addressing these issues is tempered by the realities of the healthcare environment.

## Rise of Cybersecurity Insurance Premiums

In 2025, the cost of cybersecurity insurance will rise as insurers respond to increasing breaches and ransomware attacks. Healthcare organizations without strong security measures will face higher premiums or be denied coverage, driving investment in robust cybersecurity. Those with mature defenses will secure better insurance terms, reduce breach risks, and enhance patient trust and care continuity.



## We Saw it Coming

A review on how our 2024 predictions measured up to reality.

### Increase in AI-Driven Attacks

#### Prediction

AI-driven cyberattacks will escalate in both complexity and frequency, targeting healthcare systems.



#### Outcome

A 2024 report by MIT Technology Review highlighted the growing use of AI in cybercrime, emphasizing its potential to outpace manual detection systems in speed and complexity. Cybercriminals are leveraging AI tools like generative models (e.g., ChatGPT) to enhance phishing, bypass identity checks, and create deepfakes for fraud. AI also generates malicious code and scam content, making cybercrime harder to detect and more sophisticated.

### Stronger Cybersecurity Regulations and Legislation

#### Prediction

In 2024, states are expected to introduce enhanced cybersecurity regulations, following the rollout of key national and healthcare-specific strategies in 2023.



#### Outcome

In 2024, state-level initiatives, such as New York's strengthened cybersecurity requirements that went into effect in October, further emphasized the need for robust security practices. Federal efforts to enhance healthcare cybersecurity included the Health Care Cybersecurity and Resiliency Act, which proposed grants for cyberattack prevention, training for best practices, and incident response plans.

## Growth of Telemedicine

### Prediction

The growth of telemedicine and AI generative models will expand the attack surface for cyber threats, increasing the risk of targeted attacks and potential manipulation that could harm patient outcomes.



### Outcome

Increased interconnectivity in telehealth platforms in 2024, including IoMT devices, has created more vulnerabilities for cyberattacks. The integration of wearables and remote patient monitoring has added further complexity to securing patient data.

---

## Third-party Incidents Targeting Supply Chains

### Prediction

Third-party incidents targeting healthcare supply chains are expected to intensify throughout 2024.



### Outcome

In 2024, 45% of healthcare breaches were linked to third-party compromises, creating massive supply chain issues. Notable incidents include OneBlood's ransomware attack, causing blood shortages, the BlackSuit gang's attack on Octapharma, shutting down over 190 plasma centers, and the Change Healthcare breach, which disrupted hospitals' financial operations.



# About the Contributors



**Dan L. Dodson**

CEO  
Fortified Health Security

As the CEO of Fortified Health Security, Dan Dodson brings over 17 years of experience leading healthcare and insurance organizations. Throughout his career, he has held pivotal leadership roles, including Executive Vice President at Santa Rosa Consulting, Global Healthcare Strategy Lead at Dell Services, and various leadership positions within Covenant Health System, The Parker Group, and Hooper Holmes. In 2018, Dan was recognized as a rising healthcare leader under 40 by Becker's Hospital Review, and in 2022 he was elected to the Association for Executives in Healthcare Information Security (AEHIS) Board of Trustees. As a recognized thought leader in healthcare cybersecurity, Dan is a frequent speaker at industry events and conferences including CHIME, HIMSS, and HIT Summits.

Dan's insights and data-driven expertise in cybersecurity, data privacy, risk management, and threat mitigation are regularly featured in popular media and trade publications such as Becker's Hospital Review, Healthcare Business Today, and Healthcare Innovation News.



**Paul Connelly**

Independent Board Member  
CISO

Paul has three decades in senior cybersecurity leadership roles at the White House, a big four public accounting firm, and a Fortune 100 company.

He built the first cybersecurity programs at the White House and HCA Healthcare and led them a combined 28 years in Chief Information Security Officer (CISO) roles. He also spent six years building a cybersecurity audit and consulting practice and became a partner at PricewaterhouseCoopers. Throughout, Paul has been a developer of leaders, with thirty-eight members of his teams selected for CISO positions.

Paul now focuses on raising the bar for CISO leadership. He is an independent director on the board of Fortified Health Security, technical advisor to the board of the U.S. Organ Procurement and Transplantation Network, and a developer of National Association of Corporate Directors programs. He advises and mentors CISOs as a faculty member at IANS Research; is an active cybersecurity and AI thought leader appearing in publications and conferences; and develops and teaches cybersecurity leadership programs at Belmont University.



## Russell Teague

Chief Information Security Officer  
Fortified Health Security

Russell's twenty years in Information Security spans Healthcare, Pharma, Financial, and Technology sectors. A U.S. Army Intelligence veteran and former CSO/CTO at leading cybersecurity firms, Russell's contributed his expertise to the White House's National Cybersecurity Healthcare Strategy and has been a prominent voice at major industry events, including Blackhat, HIMSS, and Health Connect Partners (HCP).



## Kate Pierce

Senior vCISO & Executive Director of Subsidy Program,  
Fortified Health Security

With over 30 years in healthcare IT and 13 in cybersecurity, Kate Pierce brings a deep understanding of improving security with limited resources. As a former CIO and CISO at a Critical Access Hospital, she built the organization's security program from the ground up. She actively collaborates with HSCC CWG and the 405(d) program and regularly advocates at federal and state levels to strengthen healthcare cybersecurity.



## Jason Myers

VP Advisory Services,  
Fortified Health Security

Jason Myers brings over 20 years of experience in healthcare, IT operations, and cybersecurity to Fortified. He previously served as Head of IT Central Services at Amazon and held leadership roles at MEDHOST, including Chief Information Officer.



## **Kenneth Bradberry**

vCISO  
Fortified Health Security

Ken Bradberry is a virtual Chief Information Security Officer for Fortified Health Security with 28 years of healthcare IT experience. Formerly CTO for Xerox Commercial Healthcare, he specializes in advancing IT operations and security solutions for healthcare providers, payers, and life sciences organizations.



## **Jake Bice**

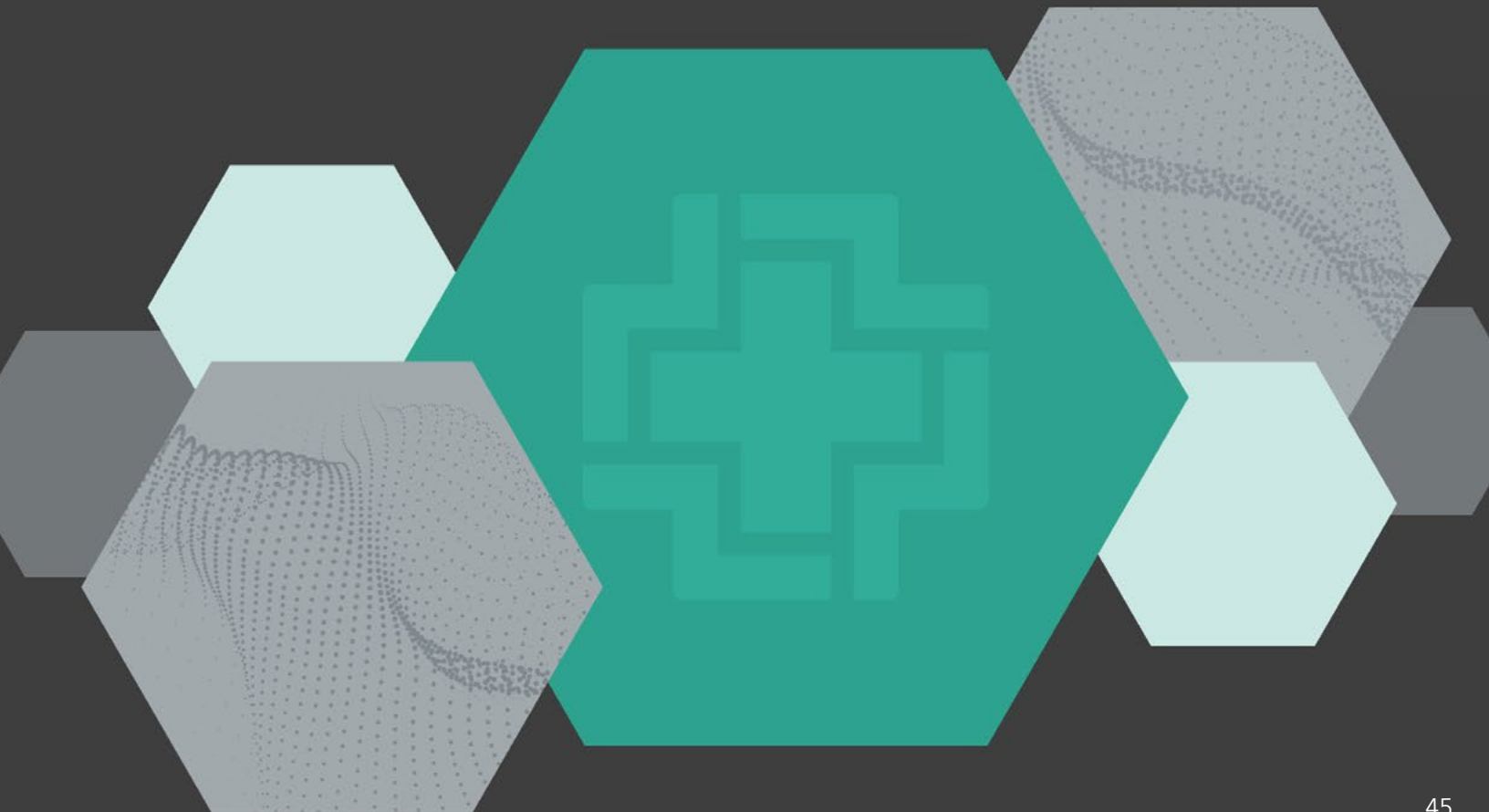
Director of Cybersecurity Operations  
Fortified Health Security

Jake Bice is the Director of Cybersecurity Operations at Fortified Health Security. In this pivotal role, Jake is responsible for the strategic oversight of the Security Operations Center, assessing and resolving client needs, training teams, and refining the processes that underpin service delivery to clients. Jake's extensive career in Infosec has been dedicated entirely to supporting healthcare environments, and his wealth of experience provides invaluable insights and context from both operational and technological perspectives.

# About Fortified Health Security

Fortified is Healthcare's Cybersecurity Partner® - protecting patient data and risk throughout the healthcare ecosystem. A managed security service provider that has been awarded many industry accolades, Fortified works alongside healthcare organizations to build customized programs designed to leverage their prior security investments and current processes while implementing new solutions that reduce risk and increase their security posture over time.

Led by a team of industry-recognized cyber experts, Fortified's high touch engagements and client-specific process maximize engagement value and deliver an actionable, scalable approach to help reduce the risk of cyber events.





[www.fortifiedhealthsecurity.com](http://www.fortifiedhealthsecurity.com)

[connect@fortifiedhealthsecurity.com](mailto:connect@fortifiedhealthsecurity.com)

120 Brentwood Commons Way  
Building 4, Suite 500  
Brentwood, TN 37027

