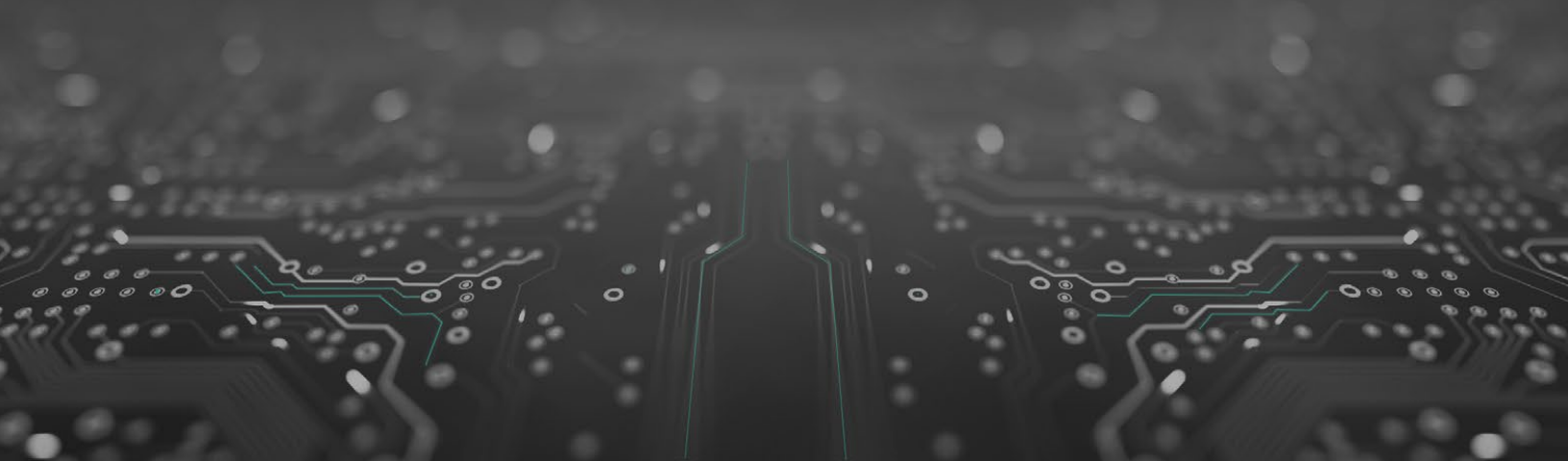
Fortified℠ HEALTH SECURITY

# 2024 HORIZON REPORT

The state of cybersecurity in healthcare



# About the **HORIZON REPORT**

The Fortified Health Security Horizon Report is a leading industry publication on cybersecurity news, trends, and guidance. Published semi-annually since 2017, our Horizon Reports are packed with valuable insights on:

- Reported data breaches and their entry points
- Evolving healthcare marketplace dynamics
- Emerging threats and threat actors
- Navigating the increasingly complex world of healthcare cybersecurity

This free report can help you and your teams stay ahead of trends and safeguard your healthcare organization against cyber attacks.

# CONTENTS



# CEO's **MESSAGE**

As we welcome and prepare for a new year, I'd like to reflect on both the progress and challenges that have shaped the healthcare cybersecurity landscape thus far.

In recent years, the healthcare industry – and even the U.S. government – has made commendable strides toward embracing a security-first mindset. Protecting health information and technology assets has become a priority, and this is undoubtedly good news. However, the less favorable development is that cyber threats against healthcare continue to grow in sophistication and increase at an alarming rate.

Over the past decade (2013-2023), more than **489 million patient records** have been compromised. And with the average recovery cost exceeding $9.48 million per breach, healthcare data breaches are officially the costliest among all industries.

Despite increased attention on the security challenges facing hospitals and health systems, the broader industry continues to struggle with significant human resource gaps, which is a crucial component to preventing cybersecurity incidents. These skill discrepancies are especially acute for organizations looking to hire individuals with *healthcare* cybersecurity expertise.

Closing these gaps, protecting patient data, and ensuring the well-being of our communities will continue to require collaborative solutions, congressional support, alternative approaches, and knowledge-sharing.

Ultimately, this mindset is at the heart of our Horizon Reports. Whether we're sharing strategies for how to reduce your cyber risk, updating you on what's happening on the legislative front, or enlightening you on the rise of AI and machine learning, we believe that knowledge is power.

**And when it comes to confronting the cybersecurity threats facing our healthcare system, we are stronger together.**

As you read the 2024 Horizon Report, we encourage you to share your feedback and perspectives with us at: connect@fortified-healthsecurity.com.

Thank you for your dedication to healthcare cybersecurity.

Regards,

Dan L. Dodson

# 2023 Year in Review

2023 data from the U.S. Department of Health and Human Services Office for Civil Rights (OCR) reveals a troubling trend in healthcare. While healthcare data breaches have declined in recent years, the number of patient records impacted has surged. Notably, third-party Business Associates (BAs) are increasingly cited as either the source of these breaches or present when they occur.

This shift is not an isolated occurrence; historical data corroborates this pattern, suggesting a significant transformation in the tactics of cybercriminals. Rather than employing a broad, indiscriminate approach to network breaches, they are now zeroing in on more specific targets.

## Number of breaches and patient records exposed

Over the past decade, OCR data reveals that there have been 5,181 reported healthcare breaches, compromising the personal health information (PHI) of approximately 489 million patient records across the United States.

In 2023, we witnessed a significant peak in patient data exposure, surpassing the previous high-water mark of 2015.

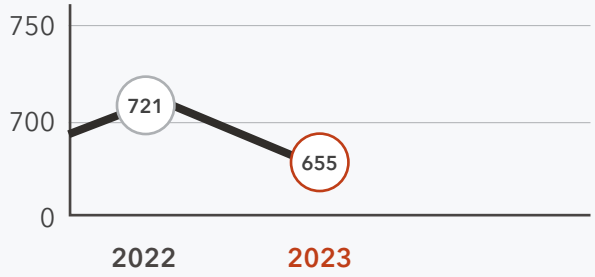
During that year, three major breaches (Anthem, Premera Blue Cross, and Excellus Health Plan) contributed to the exposure of over 112 million patient records, with nearly 100 million (88%) stemming from these breaches.

Despite this anomaly, the number of incidents and exposed patient records has risen steadily each year.

Unfortunately, over the past decade, no year had a concurrent decline in incidents and exposed records. This trend suggests that while malicious actors may shift tactics over time, their attacks on healthcare organizations will only increase.

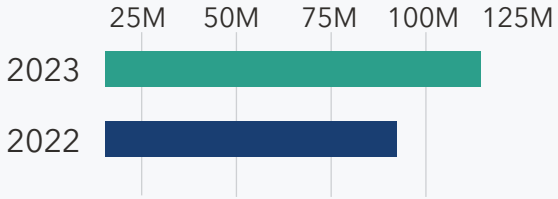
A look at year-over-year OCR data on breaches and exposed patient records brings the historical stats into focus. The total number of reported breaches declined marginally by 9% (721 – 655). However, the number of patient records exposed rose sharply to more than 116 million, a 108% Y/Y increase.

**Number of Breaches from 2022 - 2023**



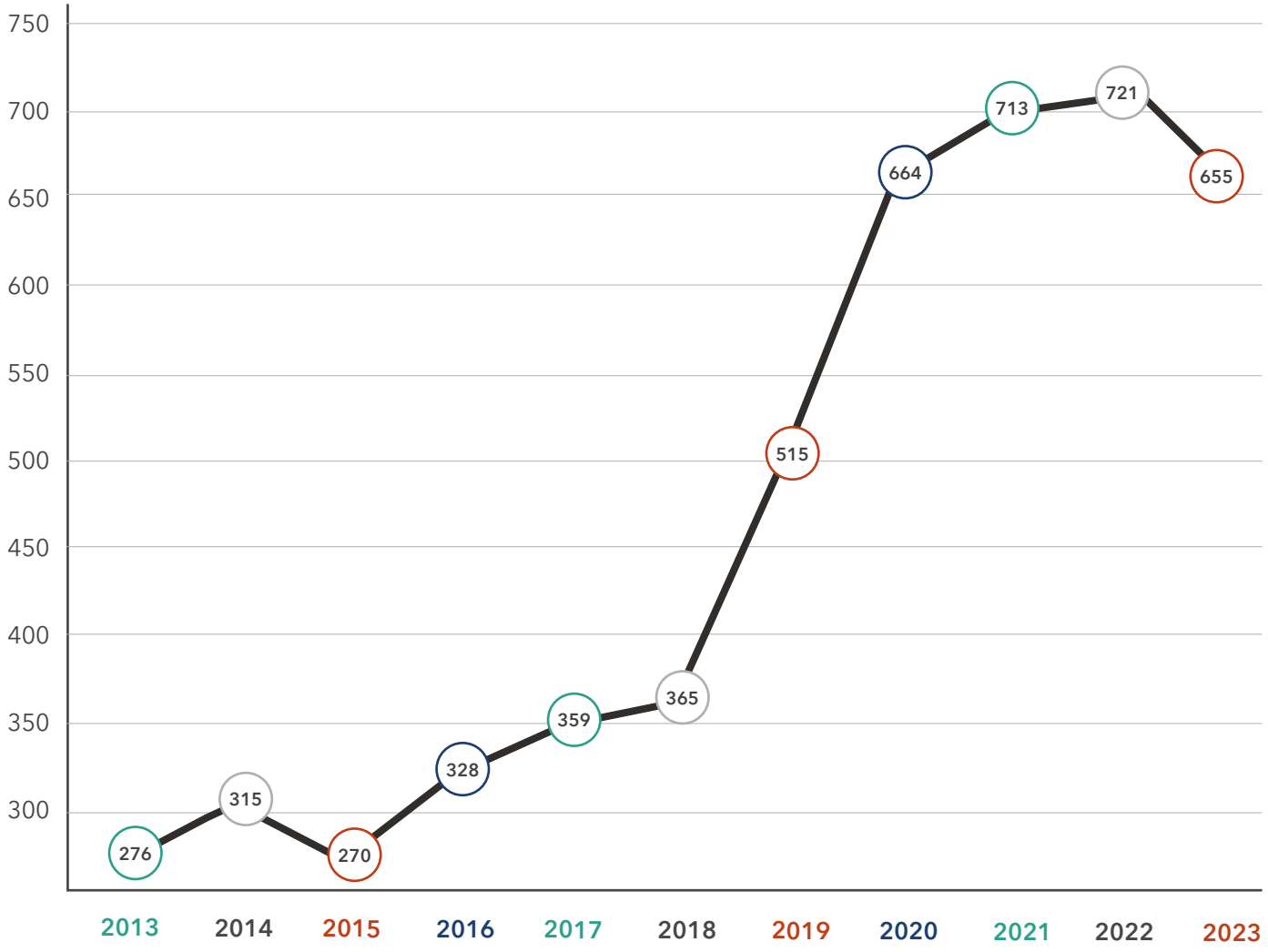

In 2022, three breaches exposed more than two million patient records each. In 2023, the number of breaches exposing more than two million patient records skyrocketed to 16. There has also been an 83% Y/Y increase in breaches exposing over a million patient records.

**Patient Records Exposed from 2022 - 2023**

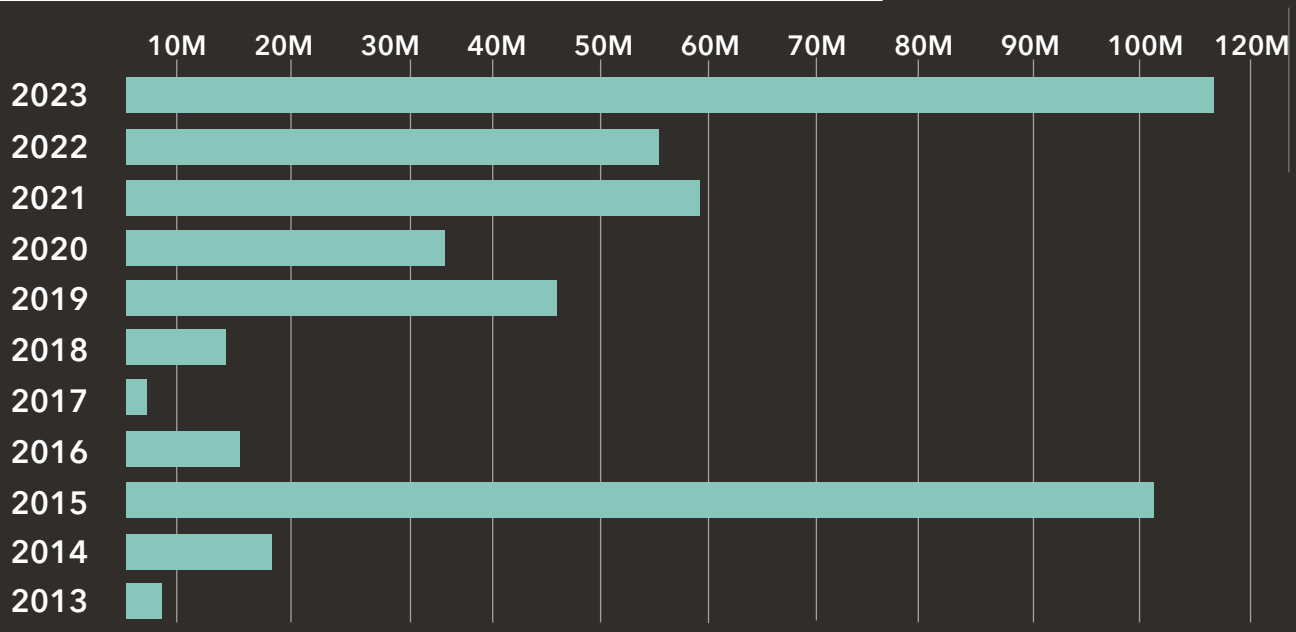



These substantial numbers indicate that when threat actors gain access, they are exfiltrating larger sets of patient records. Early detection and remediation plays a pivotal role in preventing hackers from advancing to critical network access levels or moving laterally through the network using "living-off-the-land" tactics, which can result in large-scale breaches.

## Number of Breaches 2013 - 2023

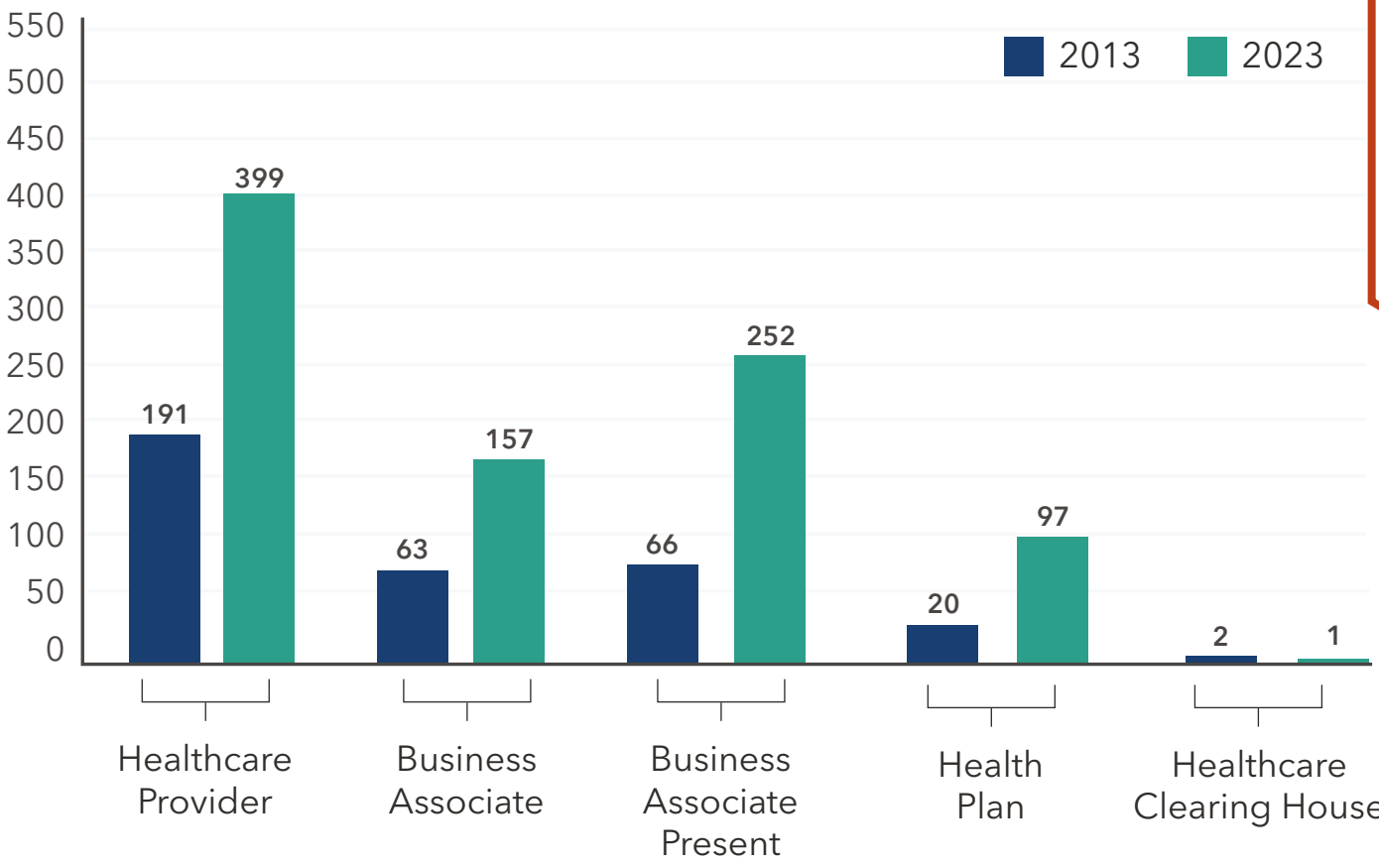



## Patient Records Exposed 2013-2023



# Type of entity reporting a breach

Between 2013 and 2023, the number of Business Associates (BAs) reporting a healthcare data breach increased by 149%. In addition, breaches directly involving BAs and breaches where BAs were present have increased by more than 217% over the past decade.




## 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 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.

## What to look for in a third-party risk management program:

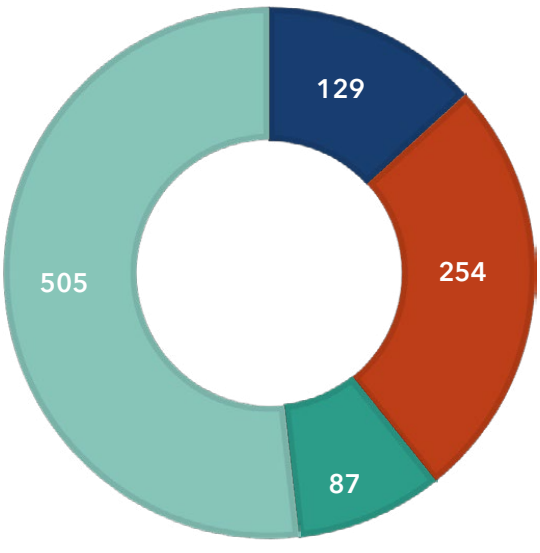
1. Thorough review and evaluation of vendors
2. Assessment of results
3. Review and evaluation of vendor documentation
4. Analysis and documentation of risk
5. Actionable results
6. Well-defined and communicated Corrective Action Plans (CAPs)

Between 2022 and 2023, Business Associate breaches increased by 22%.

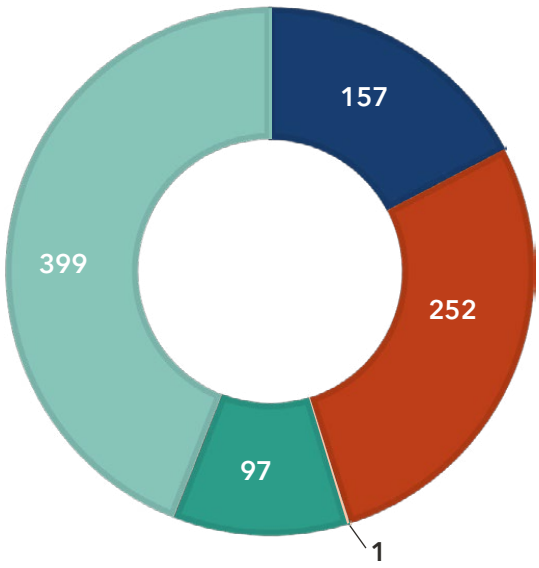
The growing presence of BAs either directly or indirectly involved in a healthcare breach underscores the criticality of having a strong third-party risk management (TPRM) program.

A robust TPRM program helps you identify and mitigate risks posed by BAs while bolstering the effectiveness of your governance program.

**Breach by Entity in 2022**




**Breach by Entity in 2023**




Business Associate

Business Associate present

Healthcare Clearing House

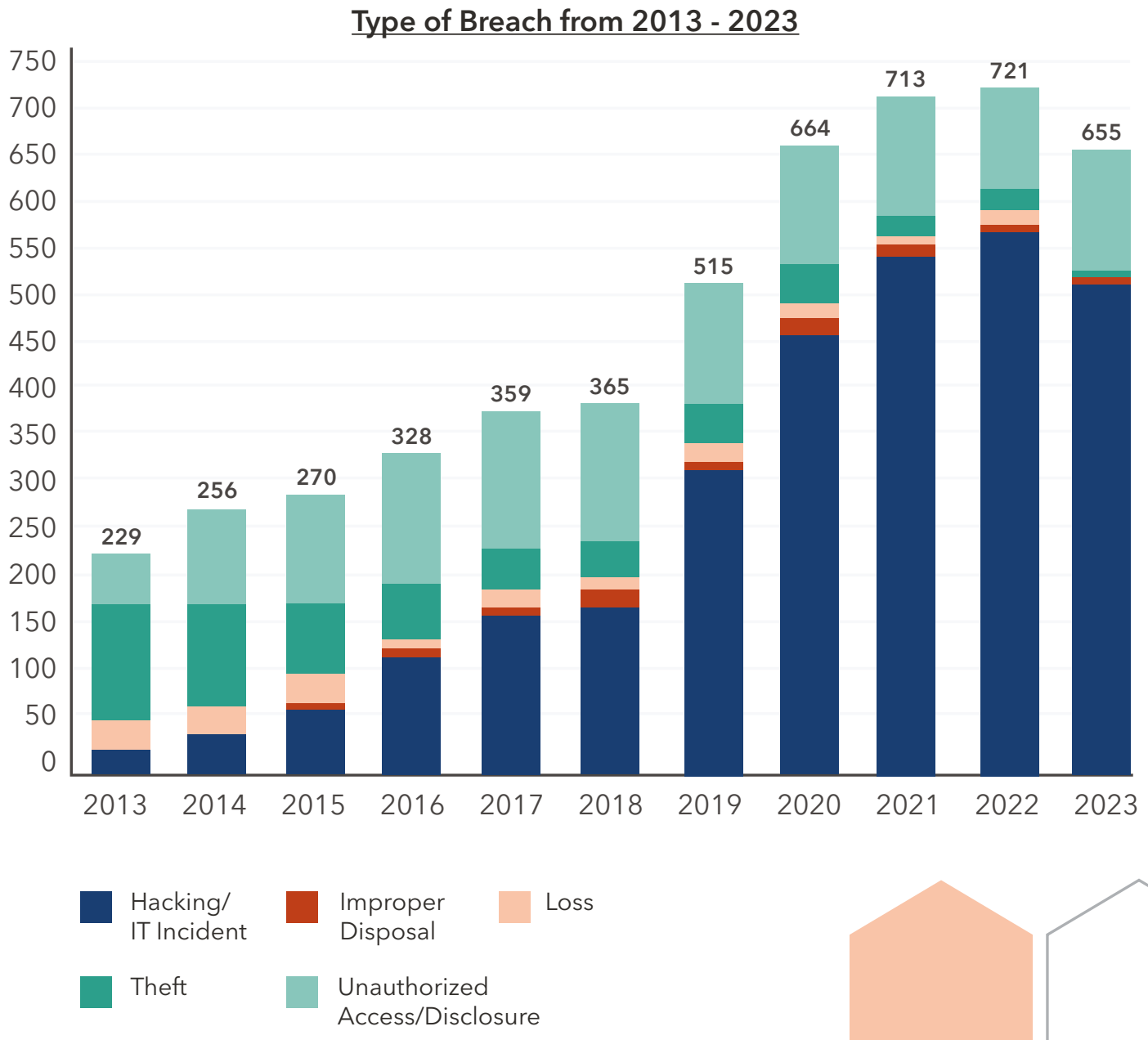
Health Plan

Healthcare Provider

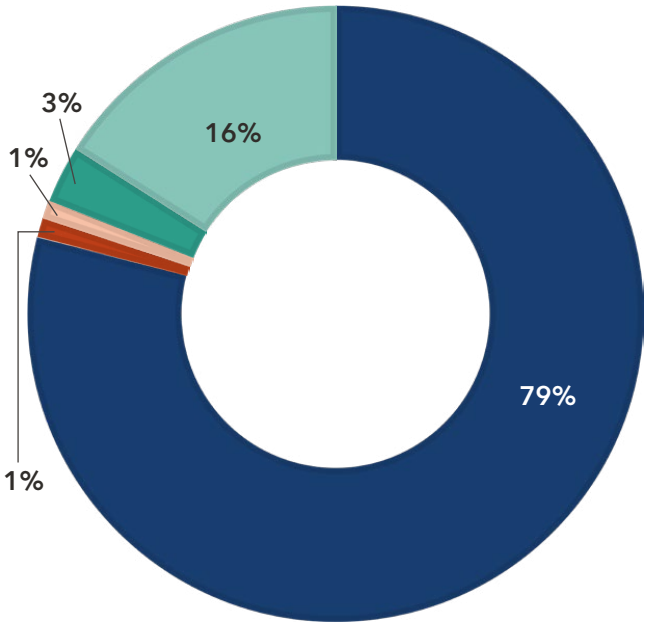
# Type of Breaches

In the last decade, breaches stemming from hacking and IT incidents have increased 1,815%, and breaches from unauthorized access and disclosures have increased 94%. Conversely, breaches resulting from the physical theft of records have declined by 91% since 2013.

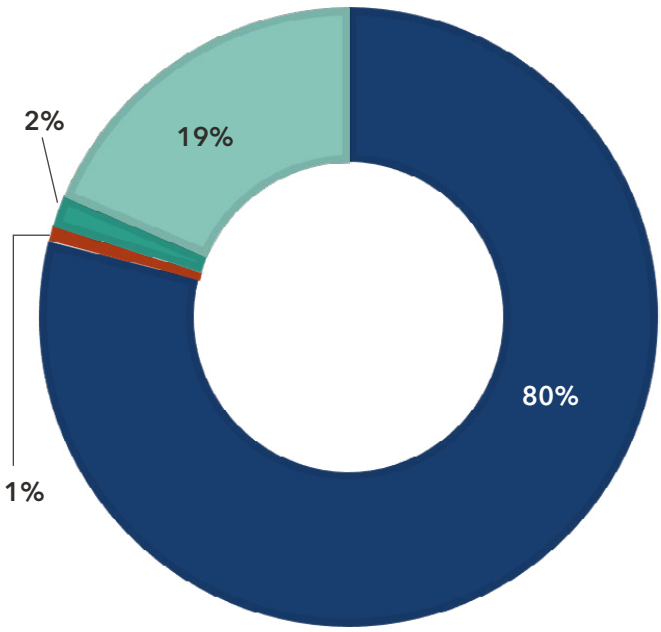
This shift can likely be attributed to the proliferation of electronic patient records and the expanded attack surface that provides more opportunities for malicious actors to target.



## Type of Breaches in 2022




## Type of Breaches in 2023




Hacking/ IT Incident

Improper Disposal

Loss

Theft

Unauthorized Access/Disclosure

## 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

Connected technologies are now the primary locations where patient records are compromised. For example, attacks on network servers (+1,272%), electronic medical records (EMR) (+29%), and email (+457%) all rose sharply compared to 2013.

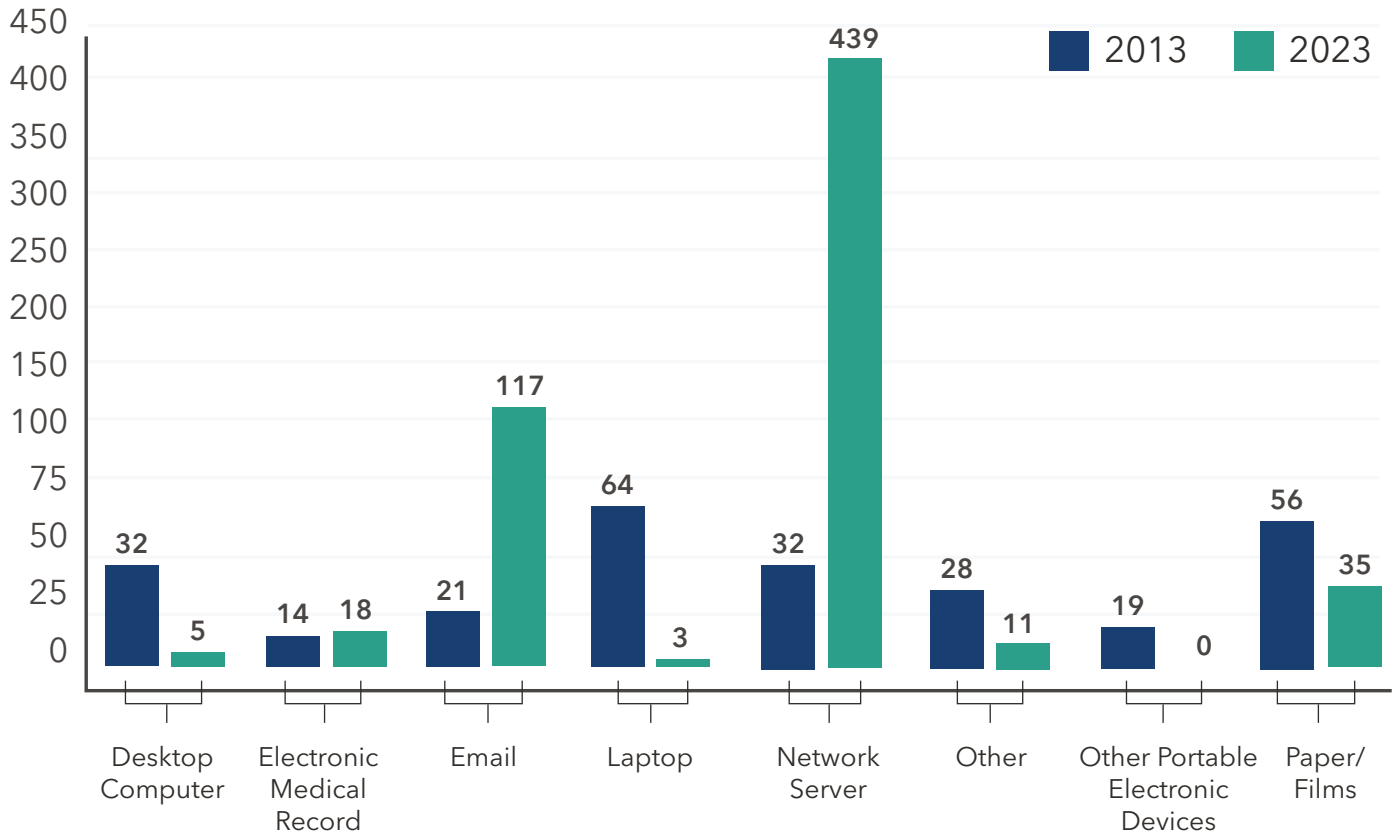
Healthcare organizations hold vast amounts of patient data beyond their EMR systems, and much of it remains alarmingly unguarded.

Based on 2023 OCR data, only 3% of breaches were located on EMR systems, indicating that the majority originated from data stored on other network connected technologies waiting to be collected and exfiltrated.

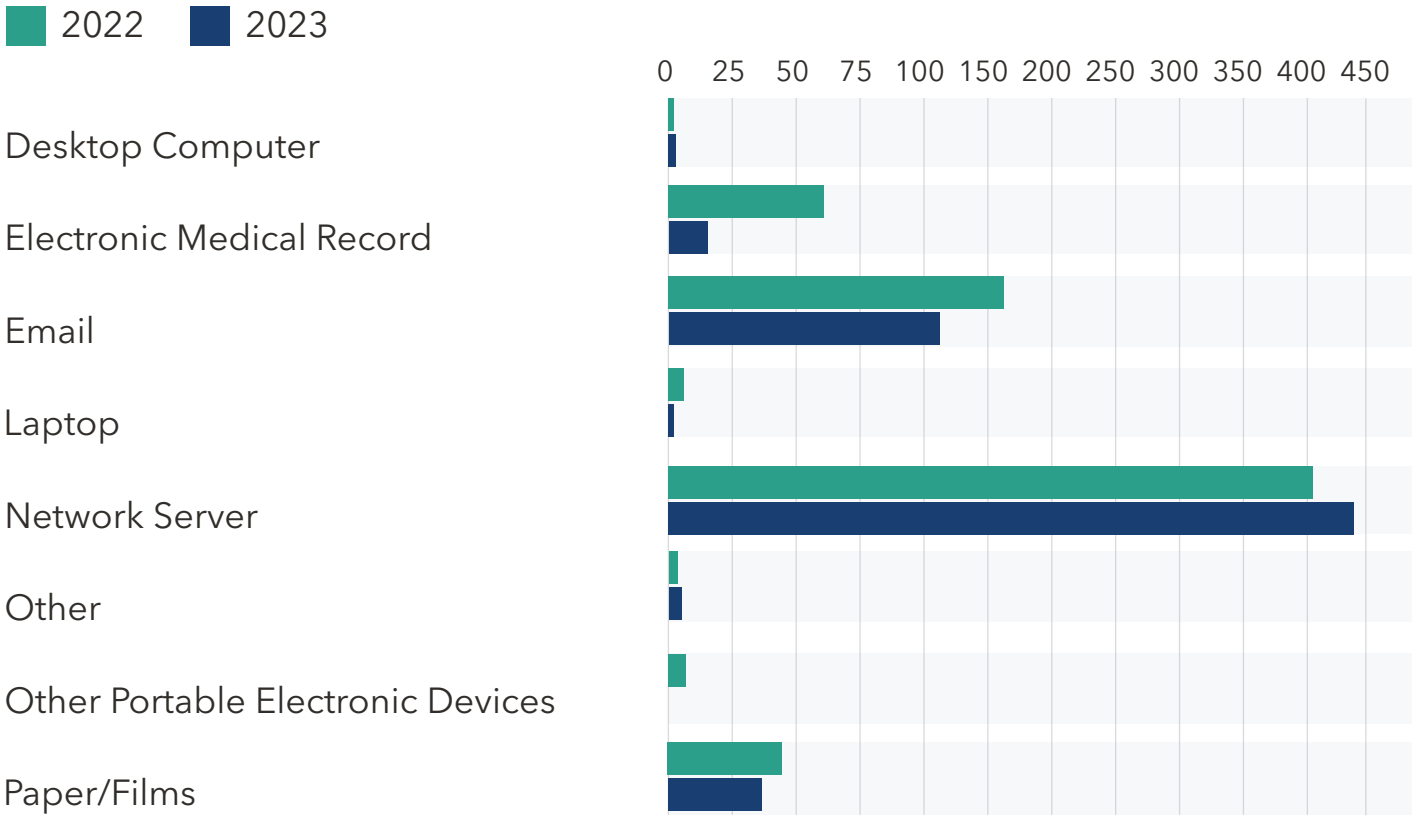
This highlights a critical need for robust Health Information Data Management.

By understanding and securing the processes that lead to these vulnerabilities, healthcare organizations can better protect their valuable data, making it more challenging for threat actors to exploit.

**Location of Breach Information 2013 vs 2023**



**Location of Breached Information 2022 vs 2023**




## Connected risks and rewards

Malicious actors have set their sights on the healthcare sector, driven by the abundance of patient information and the continuous generation of data. The risks have also spread beyond healthcare organizations to encompass third-party vendors accessing patient data to help facilitate care.

In light of the uptick in breaches involving Business Associates (BAs) and the substantial rise in breaches in 2023 affecting two million records or more, it's imperative for healthcare cybersecurity programs to adapt. Third-party risk management, incident response planning, and strengthening your culture of cybersecurity are pivotal to addressing and mitigating rising threats to our healthcare system.

# Strategic Solutions for **Reducing Cybersecurity Incidents**

From legal and regulatory penalties to reputational damage, a cybersecurity breach can have serious ramifications for a hospital and its patients. The insights and recommendations in this section are designed to equip you with knowledge and strategies that can help safeguard your organization and protected health information.

## Designing Impactful Tabletop Exercises for Safety, Security, and Preparedness

As healthcare organizations strive for a resilient and robust defense against cyber attacks, tabletop exercises (TTXs) emerge as a strategic, practical, and proactive solution.

> Beyond merely being a preventive tool, a TTX stress-tests the alignment of people, processes, and technology, offering a prescriptive lens through which organizations can gauge and enhance their incident response efficacy in real-time scenarios.

These exercises help organizations prepare for real incidents by identifying strengths and weaknesses in their response plans without the pressure of an actual emergency.

Scenarios can cover everything from identifying an incident and mitigating the damage to determining processes and protocols for communicating with cyber insurance carriers and the media.

Through these discussion-based trainings, organizations can better understand their cybersecurity readiness and improve their incident response plans.

Although TTXs inherently offer substantial value, there are **10 ways that healthcare organizations can maximize their effectiveness and impact:**

## 1 Come prepared

Proper preparation for a TTX includes distributing essential documents to attendees in advance of the actual exercise, including your Incident Response Plan, Responsibilities Matrix, and procedural playbooks. The primary question you want participants to contemplate during the exercise is, "Where is the failure point?" These materials are vital to helping them explore that question and understand what the current baseline is.

## 2 Customize the experience

Healthcare environments present unique challenges to cybersecurity, and each organization has its distinct nuances and obstacles. Therefore, a generic, one-size-fits-all approach to a tabletop exercise will not be adequate or offer participants maximum value.

Regardless of whether you opt for a paid or complimentary service to conduct your TTX, it is paramount that proctors or facilitators ensure that the simulated scenario is meticulously tailored to reflect your specific environment and organizational structure. This will make the exercise more relevant, and keep participants attentive and engaged, improving the training and readiness results of the session.

## 3 Encourage candid feedback

Incident response tabletop exercises provide a unique opportunity to identify vulnerabilities and operational gaps in your incident response procedures and command structure. By encouraging participants to provide candid feedback around these areas of exposure, including inefficiencies and risks incurred by incomplete technology implementations, the individuals within your organizations can work together to close critical gaps and ensure your hospital and patients are better protected.

## 4 Test procedures

Every organization should have well-documented incident response procedures in place. Tabletop exercises allow these procedures to be tested in a risk-free environment. Participants can identify any problems or ambiguities in the procedures, ensuring they are clear, actionable, and effective. This iterative process can facilitate actual procedural improvement.

## 5 Communicate expectations

Tabletop exercises do more than just test procedures. They elevate participants' skills, strengthen their incident response readiness, and help clarify what additional duties they might need to perform during a real incident. The ultimate goal is to help participants develop their problem-solving skills, effectively collaborate and coordinate, and adapt to dynamic and evolving situations. To ensure participants are aligned on this, it's essential to communicate these goals and expectations with them before, during, and after a tabletop exercise is conducted.

## 6 Shake up the scenario

Effective incident response requires quick and critical thinking, often under pressure. To help encourage group collaboration and critical thinking as participants devise solutions to simulated incidents, consider engaging participants in a scenario where they are asked to devise strategies without relying on the standard approach or the expertise of a particular individual or group, assuming they are unavailable. Such hypothetical situations can inspire innovative solutions and encourage adaptive problem-solving skills.

## 7 Identify your key players

In the chaos of an actual incident, it's essential to know who the key players are within your organization. Tabletop exercises can help with identifying who these individuals are and understanding the role(s) that they play, enabling swifter decision-making and communication during a crisis.

## 8 Expand the circle

Involving individuals outside the core IT and leadership teams, such as clinical and operational staff, is another way to maximize the value of your TTX. Inviting them to not only observe the training but also inquire about how they can assist, can ensure a holistic response strategy. Even though some might be unsure of how to contribute, assistance is seldom disregarded during crises.

## 9 Clarify your communications

Tabletop exercises facilitate swift information dissemination to crucial internal and external stakeholders, including patients, vendors, partners, and regulatory entities, and ensure it's tailored to the incident type. TTXs also act as a conduit to educate team members about robust communication protocols, outlining how to report incidents, identify contacts, and determine what information to relay. Consider testing your notification procedure to the TTX, so participants can integrate recent practical experience into the exercise.

## 10 Double down on documentation

During an incident, access to critical documentation is essential. Tabletop exercises can reveal gaps in documentation, helping organizations identify what information and resources are needed during downtime. This proactive approach ensures that the necessary documents and tools are readily available when they are most needed.

During your TTX, it can be invaluable to assign a scribe. Amidst discussions, this individual can help capture what potential updates need to be made to policies, procedures, and plans.

## Strengthening your cybersecurity culture

In today's threat landscape, the value of tabletop exercises cannot be overstated. Integrating TTXs into your training strengthens the culture of cybersecurity within your healthcare organization, sets your employees up for success in the event of a security breach, and helps fortify your organization's reputation and bottom line.

For information on tabletop exercises, review NIST SP 800-84.

## Safeguarding Against Cyber Incidents: Effective C-Suite Communication

Think back to the last time you presented to your hospital's executive team (C-Suite) or board of directors about your cybersecurity program. Did their eyes glaze over? Did they keep glancing at the clock, seeming to count the seconds until you were done?

Developing the skills to effectively communicate with your healthcare organization's executive team and board can be one of the most impactful things you do as a healthcare cybersecurity leader. This is because when a cyber incident occurs, it affects everyone in the organization.

Unless your leadership has experienced a cyber incident, they may not fully grasp the magnitude of its impact. And without their support, your IT team will likely be left unprepared for inevitable cyber threats.

Educating and engaging your executive team and board about the collective responsibility of cybersecurity can be challenging for cybersecurity leaders.

Here are **three strategies to help you better communicate with your hospital leadership team,** get them engaged, and reduce your organization's risk of a cyber incident:

## 1. Speak their language

In many healthcare organizations, some executive leaders and board members may not possess a robust technical background. Consequently, navigating through a cybersecurity presentation teeming with technical jargon could result in a disengaged audience.

The objective of these presentations is not to showcase your intelligence or establish your expertise in cybersecurity. Rather, it's about succinctly communicating critical points using language and concepts that resonate with your organization's leadership.

To communicate more effectively, adopt the mindset of the C-Suite and curate your presentation to cater to a business-centric perspective, not a technical one.

Place yourself in their shoes. What information would be pivotal for them to know? If impacted by a cyber incident, what might the financial implications be? What could that mean for the organization's bottom line and overall risk profile? How will it impact employees, patients, and the organization's reputation?

By using concepts and messaging that they understand, you'll be better equipped to frame your message in a way that will resonate with them while helping you accomplish your end goal: reducing the risk of a cyber incident.

## 2. Build a strategic alliance

One of the best approaches to improve how you communicate with your executive leadership team is to foster a collaborative relationship with one or more of its members. This can help you bridge the gap between technical and business perspectives, ensuring that important messages are conveyed and received.

Practical steps for strategic alignment with your leadership team:

- Identify a leader (C-Suite or board member) who shows interest in your area and is open to collaboration and mutual learning
- Share initial concepts, drafts, or outlines of your presentation, and be open to feedback and suggestions
- Ensure that their feedback is meaningfully incorporated, highlighting the parts you adjusted to incorporate their input
- Acknowledge the guidance and input of the leadership member in formal communications or presentations, demonstrating that you're fostering a culture of collaborative synergy between your cybersecurity efforts, and the health and well-being of the organization and its patients
- Make this collaboration continual, and not just a one-off event. Consistent interaction ensures that you are always in tune with the strategic orientation and current priorities of the leadership team.

### 3. Show, don't just tell

Connect the dots between the perils of a cyber incident and its potential ramifications on the business through examples and storytelling.

For example:

- Show the direct correlation between the severity of a cyber incident and the increased risk to the organization, including potential operational disruptions, damage to reputation, and revenue loss
- Address the consequences of the CEO being spotlighted in the news due to the organization experiencing a cyber incident

This is not to say that you shouldn't show metrics or data. If you have meaningful numbers that can help you illustrate a point more effectively, share them. However, at the end of the day, you'll be far more effective at engaging your audience by telling a story to make your case or get your point across.

Stories are not only more interesting to listen to, they tend to leave a stronger impression and be more effective at helping your audience understand and remember your message than just relying on data-focused slides.

## Empower your hospital leadership

**The first cyber-related discussion with your C-Suite should not occur during an incident.** Instead, it should be an ongoing conversation where they are provided with just the right amount of information to comprehend the cyber risks facing the organization.

Help them visualize the evolving cyber threat landscape, translate what those shifts mean for the organization, and convey how you're navigating these risks with a robust strategy.

Through productive and engaging information exchange, strategic insights, and clear, straightforward solutions, you empower your leadership team to effectively steer the organization through the complexities of healthcare cybersecurity, stand united, and collectively resolve issues should a cyber incident occur.

# What's on the Horizon?

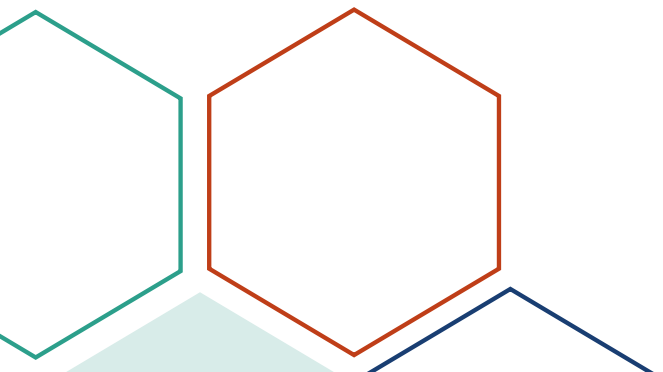
The year 2024 promises to be a critical juncture in healthcare cybersecurity, marked by the growing urgency to protect patient data, ensure the integrity of medical systems, and navigate a complex regulatory landscape.

Legislative efforts that were set in motion in 2023 may help strengthen healthcare cybersecurity, but what will that entail in 2024 and beyond? And what role will artificial intelligence (AI) play in healthcare technology?

## The Legislative Landscape Shaping Healthcare Cybersecurity

Throughout 2023, the White House elevated their efforts to address the risks associated with cyber attacks targeting healthcare and other critical infrastructure sectors.

This concerted endeavor resulted in the release of several significant documents and pieces of legislation. One such pivotal document was the National Cybersecurity Strategy, which outlines the essential concepts needed to strengthen and reshape our current cyber landscape.



This landmark document was followed by several other key releases, including the:

- National Cybersecurity Strategy Implementation Plan
- U.S. Department of Health and Human Services (HHS) Healthcare Sector Cybersecurity Strategy
- National Cyber Workforce and Education Strategy
- Announcement of upcoming revisions to the NIST framework (NIST CSF 2.0)
- Revision to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- Release of Senator Bill Cassidy's white paper on artificial intelligence
- New York State's proposed cybersecurity requirements for hospitals

As we embark upon a new year, it's important to understand what these legislative efforts entail, and how they might impact your healthcare organization in 2024 and beyond.

# National Cybersecurity Strategy Implementation Plan (NCSIP)

The National Cybersecurity Strategy Implementation Plan provides a roadmap of 69 key initiatives addressing the **five pillars of the strategy**:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

Each of these pillars were given a target completion timeline within the next three years. The chart below outlines a few items within the implementation plan that will impact healthcare along with their target due dates:

| Initiative Number | Description | Target Date |
|---|---|---|
| 1.1.1 | Establish an initiative on cyber regulatory harmonization | 1Q FY24 |
| 1.1.2 | Set cybersecurity requirements across critical infrastructure sectors | 2Q FY25 |
| 1.4.2 | Issue final Cyber Incident Report for Critical Infrastructure Act (CIRCIA) rule | 4Q FY25 |
| 3.2.2 | Initiate a U.S. Government IoT security labeling program | 4Q FY23 |
| 3.3 | Shift Liability for Insecure Software Products and Services | 2Q FY24 |
| 3.3.2 | Advance software bill of materials (SBOM) and mitigate the risks of unsupported software | 2Q FY25 |
| 3.4 | Use Federal Grants and Other Incentives to Build in Security | 4Q FY23 |
| 3.6 | Explore a Federal Cyber Insurance Backstop | 1Q FY24 |
| 4.6 | Develop a National Strategy to Strengthen Our Cyber Workforce | 2Q FY24 |

# U.S. Department of Health and Human Services (HHS) Healthcare Sector Cybersecurity Strategy

In response to the National Cybersecurity Strategy Implementation Plan, HHS published the cybersecurity strategy for the healthcare sector in early December 2023. The HHS strategy has four concurrent components:

1. Formalize essential and enhanced Cybersecurity Performance Goals (CPGs) for the health sector. These CPGs are based on the Cybersecurity and Infrastructure Security Agency's (CISA) CPGs in conjunction with the Healthcare Industry Security Practices (HICP) document published by 405d.

   **We expect that a 60-day rule-making comment period will likely begin in early 2024.**

2. HHS will work to secure upfront and ongoing incentives to help healthcare organizations implement and grow their cybersecurity programs

3. HHS will coordinate with the Center for Medicare and Medicaid Services (CMS) and the Office of Civil Rights (OCR) on setting requirements, including enforcement and accountability, and updates to the HIPAA Security Rule in the spring of 2024

4. The harmonization of the various government healthcare components into a single "one-stop shop" for cybersecurity support, naming the Administration of Strategic Preparedness and Response (ASPR) as the lead agency

As this healthcare cybersecurity strategy unfolds, it'll be essential for healthcare organizations to stay engaged with what it will mean for their cybersecurity program. This awareness and understanding will also facilitate access to potential financial incentives that may become available.

# National Cyber Workforce and Education Strategy (NCWES)

In 2023, the United States grappled with a staggering shortfall of over 480,000 unfilled cybersecurity positions. With the threat landscape expanding and cyber attacks on the rise, there emerged an urgent imperative for a unified effort to bolster the talent pool of cybersecurity professionals, especially within healthcare cybersecurity.

A critical step was taken in July 2023 with the release of the National Cyber Workforce and Education Strategy. This strategic document outlined **four essential pillars aimed at effectively addressing the talent shortage:**

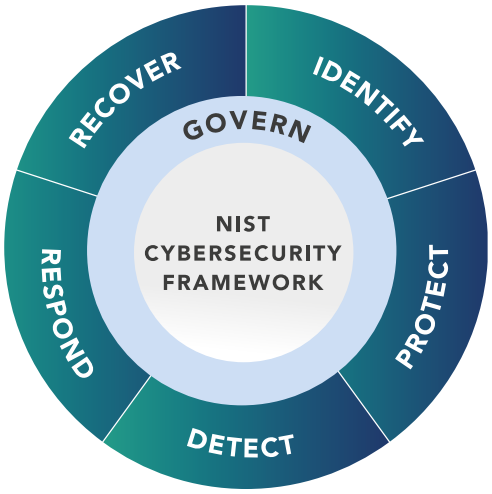
1. Equip Every American with Foundational Cyber Skills
2. Transform Cyber Education
3. Expand and Enhance America's Cyber Workforce
4. Strengthen the Federal Cyber Workforce

The Office of the National Cybersecurity Director (ONCD) has assumed the responsibility of developing the implementation plan for this strategy, including defined timelines and actionable initiatives.

As this strategy takes shape, anticipate a noticeable expansion in opportunities to engage staff in cyber education programs.

## NIST CSF 2.0

Another significant change on the horizon is the NIST CSF Framework. The most anticipated adjustment involves the addition of a sixth pillar, incorporating Governance as a fundamental new requirement that's embedded within each of the original five domains: **Identify, Protect, Detect, Respond, and Recover**.




The estimated timeline for implementation is early 2024.


Credit: https://www.nist.gov/.

## Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Although CIRCIA was signed into law in March of 2022, the target for the final implementation of this rule is now the fourth quarter of 2025. This implementation will establish stringent requirements for the timing of reporting cyber incidents to CISA, as well as specific timelines for federal entities that receive cyber incident reports to share the information with CISA. These new rules will also extend to the disclosure of ransomware payments.

Once the final requirements are in place, organizations will need to update their Incident Response Plans (IRPs) to ensure they align with the evolving regulatory landscape.

## Congressional framework for the future of AI

AI was a prominent and dynamic topic throughout 2023. The proliferation of use cases for this technology occurred so rapidly that even CEOs of leading artificial intelligence companies repeatedly met with Congress to engage in discussions about establishing "guardrails" on AI without impeding innovation.

Current regulations are still in the development phase, and Senator Bill Cassidy actively sought public input to better understand the benefits and potential risks associated with integrating AI into criticalinfrastructure businesses.

This was especially pertinent in the healthcare sector, where the primary concern revolved around potential impacts of artificial intelligence on patient safety. In response to the Request for Information (RFI), CHIME underscored crucial aspects pertaining to patient safety, privacy, security, bias, and innovation, among other concerns.

## Executive Order on AI

On October 30th, 2023, the White House released a 111-page Executive Order (EO) on the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." The goal is to establish a framework that sets guardrails around AI.

The EO contains eight guiding principles and priorities in the development of AI regulations:

1. AI must be safe and secure
2. Promote responsible innovation, competition, and collaboration
3. Support American workers
4. Advance equity and civil rights
5. Protect the interest of Americans using AI in their daily lives
6. Protect Americans' privacy and civil liberties
7. Manage risks from the Federal Government's use of AI
8. Allow the U.S. to lead the way to global societal, economic, and technological progress

The order then breaks down these principles into eleven sections of detailed, actionable steps with target dates ranging from 30 to 365 days from the date of the order. Stanford University has created a tool to track the progress of the order, with sections 4.2 and 4.3 particularly relevant to cybersecurity.

## New York State's proposed cybersecurity requirements for hospitals

New York became to first state to announce their plan to implement requirements for all hospitals within the state, accompanied by a proposed $500 million to assist in implementation.

These requirements were posted on December 6th, 2023, followed by a 60-day comment period prior to becoming law. Once published, hospitals will have one year to comply with the standards.

The requirements include:

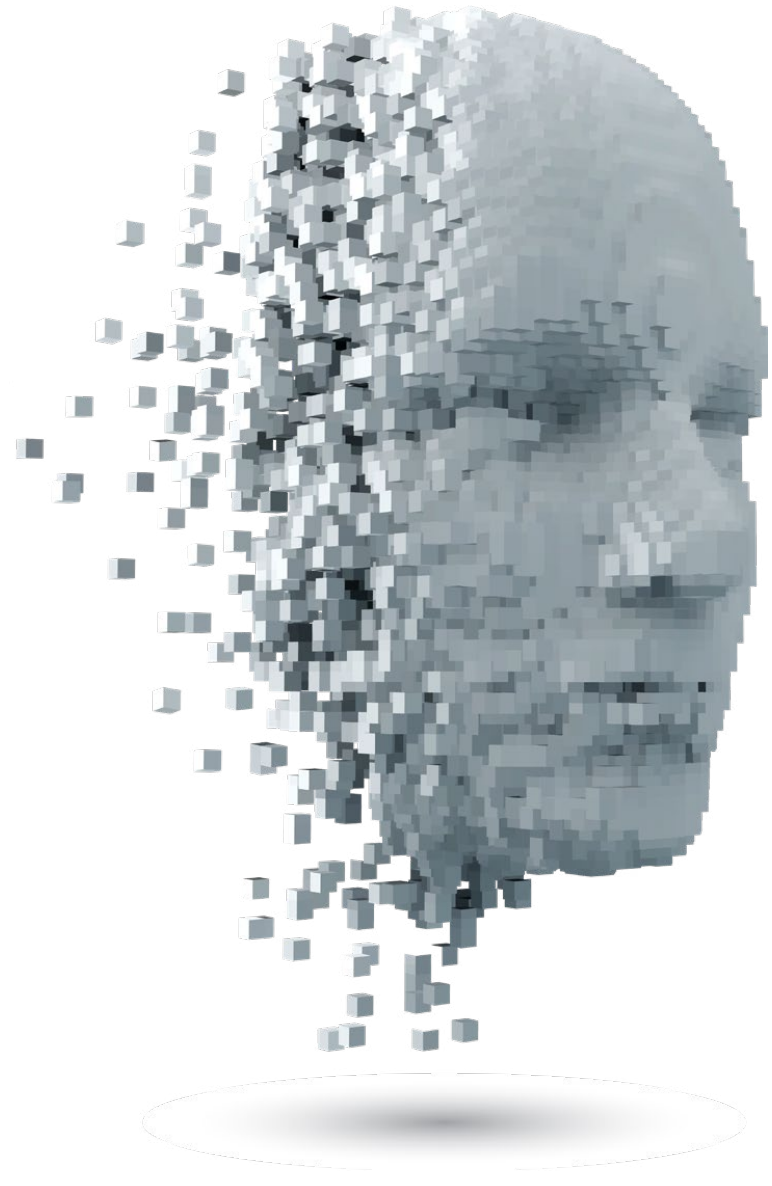
- An annual risk assessment that has a clear corrective action plan
- Early detection of cyber events with response
- Establishing an internal or external chief information security officer (CISO)
- Monitoring and testing of the cyber program
- Managing third-party risks
- Multifactor authentication
- Cyber awareness training
- An incident response plan
- Reporting an incident within two hours to the state DOH

The expectation is that these requirements will become law in New York in 2024, and that other states will follow their lead in adopting statewide cybersecurity standards for hospitals.

## 2024 legislative outlook: Building on 2023's progress

Reflecting on 2023, we anticipate a dynamic legislative landscape awaiting us in 2024. As we witness the emergence of the new National Cybersecurity Strategy, it underscores the importance of healthcare organizations collaborating to elevate our collective cyber hygiene, adopting a proactive cybersecurity stance, and securing sufficient funding.

With these challenges and opportunities on the horizon, 2024 promises to be a year of crucial advancements in safeguarding our digital landscape.



## Artificial Intelligence and Machine Learning in Healthcare: Making Informed Technology Choices

Artificial intelligence (AI) took center stage in 2023. While undeniably groundbreaking, the new, widespread adoption of this technology has triggered concerns throughout multiple industries, including cybersecurity.

In preparation for the year ahead, it's important to understand what AI truly means in the context of cybersecurity and technology. This knowledge can foster more constructive conversations within your organization, refine your evaluation of cybersecurity tools, and help you determine where AI can be beneficial and where it might pose security risks.

## What does artificial intelligence actually mean?

"Artificial intelligence" may be the new buzzword dominating headlines and cyber tech pitches, but it's a broad concept that's been around for decades. The actual term is attributed to John McCarthy, who coined it in a proposal for a workshop on "artificial intelligence."

Today, artificial intelligence (AI) refers to multiple technologies and approaches, and not all AI systems are the same. This is especially true when one compares AI with its often conflated counterpart, "machine learning" (ML).

**The unique characteristics of each – AI and ML – are garnering both enthusiasm and concern, especially in relation to emerging healthcare technologies.**

However, it's important to understand their true significance and the potential they hold to influence, or even disrupt.

## Artificial intelligence vs machine learning

When thinking about AI vs ML, consider a toolbox. AI would be the box containing a variety of tools, whereas ML would be a trusty hammer within that toolbox.

AI encompasses computer systems capable of performing tasks that typically require human intelligence. This includes creating algorithms and models that allow machines to imitate cognitive functions like learning, problem-solving, and decision-making.

Machine learning, on the other hand, is a subset of AI with a specific approach. It focuses on enabling machines to learn from data without being explicitly programmed.

## The significance for healthcare organizations

Understanding the difference between true AI and ML is crucial for healthcare organizations, especially when evaluating technology vendors. Many vendors claim to offer AI-based tools, but it's essential to discern whether they are referring to true AI or ML. This distinction can impact the capabilities and limitations of the tools.

Moreover, healthcare organizations often share sensitive data with technology vendors for analysis and insights. It is vital to comprehend how vendors use this data and ensure compliance with privacy regulations. A thorough understanding of a vendor's data practices, as well as third-party risk management processes, can influence decision-making when selecting a vendor.

By incorporating third-party risk management, healthcare organizations can better assess and mitigate potential risks associated with vendor relationships, safeguarding their sensitive data and maintaining compliance with privacy regulations.

**To better understand and manage the potential risks associated with using AI-based tools in your environment, here are a few questions to consider:**

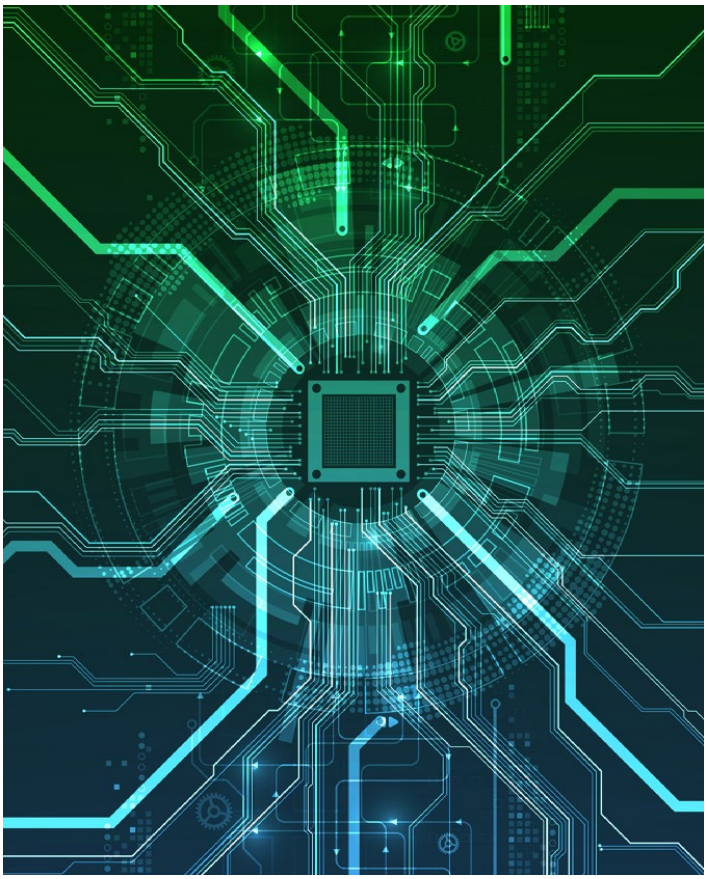
- How many of our vendors use AI or ML to some extent?
- For the vendors using AI or ML, how does each solution use my data to train its system? And how does the vendor treat my data once training is completed?
- What data do the vendors listed above have access to?
- Do any of the agreements I signed with the vendors outline the data requirements needed or the process by which the vendor will be responsible for the mishandling of my data?

## Using AI safely and securely

As noted in our Legislative Landscape section above, an Executive Order was issued in the fall of 2023 to help ensure that AI is safe, secure, and trustworthy.

Specific sections of this EO also include directives to federal agencies to develop standards and address the risks that it may pose to chemical, biological, radiological, nuclear, and cybersecurity systems.

For example, the executive order directs the Defense Department and the Department of Homeland Security to conduct a pilot project using AI capabilities to help find and remediate vulnerabilities in the federal government's software, systems, and networks.



Many AI experts, industry groups, and companies welcomed the EO as an important step forward, praising the inclusion of fairness, privacy, and the need for testing before launching new AI tools. Aligned with these initiatives, Fortified led an AI focus group at CHIME Fall Forum in November 2023, and has spearheaded an AI working group in collaborating with healthcare cybersecurity leaders to develop an AI governance model for healthcare organizations.

# Cybersecurity Outlook for 2024

Key areas to watch in the coming year.

## What We Expect to See in 2024

### 1. Increase in AI-driven attacks:

As the use of artificial intelligence (AI) by malicious actors increases, attacks on healthcare will also increase in their sophistication and volume. In response, healthcare organizations will prioritize the development of AI governance in their effort to fortify their defenses. A greater focus will also be given to the art and science behind "training the people" through security awareness training programs to help identify and prevent these types of attacks.

### 2. Stronger cybersecurity regulations and legislation:

In 2023, increased cybersecurity regulations and strategies were rolled out, including the National Cybersecurity Strategy Implementation Plan and the Healthcare Sector Cybersecurity Strategy. New York state legislators also announced groundbreaking cybersecurity legislation for hospitals in the state. In 2024, we expect other states to introduce similar legislation, strengthening cybersecurity across various sectors.

### 3. Telemedicine:

With the expansion of telemedicine services, the attack surface for cyber threats is broadening, increasing the likelihood of these platforms becoming targets for cyber attacks. In addition, increasing use of AI generative models will likely lead to threat actor bias manipulation, resulting in harm to patient outcomes.

### 4. Supply chain cybersecurity:

The trend of threat actors targeting healthcare supply chains, including business associates and third-party vendors, has increased over the last few years. We anticipate third-party incidents will continue to increase in intensity throughout 2024.

# Were We Right?

Each year, we take a moment to reflect on our previous year's predictions and compare them with what happened. Here's a look at Fortified's 2023 predictions:

## Increased cybersecurity funds for providers

**Prediction:** We expect additional funding support for continuing efforts to help healthcare organizations secure their technology infrastructure.

**How did we do?** Fortified's discussions with the White House have indicated that future funding is on the horizon. Significant progress has been made under the National Cybersecurity Strategy Implementation Plan at both federal and state levels, and there's a growing consensus that funding is essential for the sustained advancement and continued maturity of healthcare cybersecurity initiatives.

## Cybersecurity spending will increase

**Prediction:** Backlogged or delayed cyber projects can't wait any longer. Despite increased revenue and expense pressure on hospitals and health systems, higher spending on cybersecurity is expected in 2023.

**How did we do?** Our internal research indicates a rise in investment in both in-house IT security departments and external partnerships. Moreover, the valuation of the U.S. healthcare cybersecurity market across all industries has grown from $4.86 billion in 2022 to $5.65 billion in 2023. Notably, the healthcare provider segment accounts for the largest portion of this domestic market's revenue.

## Expect more large-scale breaches

**Prediction:** While the overall number of breaches will be steady or slightly higher, we foresee a rise in large-scale breaches like the CommonSpirit Health breach in October.

**How did we do?** OCR data reveals a dramatic rise in significant breaches, with 16 incidents in 2023 exposing over two million patient records each. Furthermore, there's been an 83% Y/Y increase in breaches that have exposed over one million patient records per incident. This data indicates that large-scale breaches were a reality in 2023, impacting a larger number of patients in the process.

## Continued IT talent crunch brings more MSSP partnerships

**Prediction:** IT talent challenges will accentuate the value of partnering with a managed security services provider to handle day-to-day cybersecurity tasks and more sophisticated deployments while supplementing existing IT staff.

**How did we do?** At Fortified, we've seen a notable increase in requests for staff augmentation and Expertise on Demand services throughout 2023, a trend reflected throughout the healthcare cybersecurity ecosystem.

# 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*.

**WILLIAM CRANK**
*Chief Operating Officer*
Fortified Health Security

Throughout his distinguished career, William Crank has been at the forefront of developing and implementing robust cybersecurity strategies tailored for the healthcare sector. His leadership roles have included overseeing the Information Security Risk Management (ISRM) team at Hospital Corporation of America (HCA) and serving as Chief Information Security Officer (CISO) at MEDHOST.

He has held numerous certifications in the areas of Information Security and Information Technology, has served as Sponsorship/Programs Director and Vice President of the Middle Tennessee chapter of the Information Systems Security Association (ISSA), and retired after serving more than 20 years in the United States Navy.

**RUSSELL TEAGUE**
*Chief Information Security Officer*
Fortified Health Security

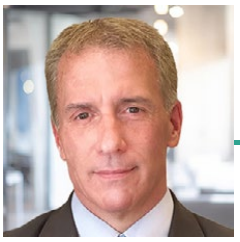
Russell's twenty years in Information Security spans Healthcare, Pharma, Financial, and Technology sectors. A U.S. Army Intelligence veteran and former CSO/CTO at leading cybersecurity firms, Russell's contributed his expertise to the White House's National Cybersecurity Healthcare Strategy and has been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

**KATE PIERCE**
*Senior vCISO & Executive Director of Subsidy Program*
Fortified Health Security

With over 30 years of experience in healthcare information technology, and over 13 years in healthcare cybersecurity, Kate Pierce has deep insight into the persistent challenge of improving security with increasingly limited resources. During her tenure as the CIO and CISO at a Critical Access Hospital, Kate spearheaded the creation of the organization's security program, encompassing governance, strategic planning, and the selection and rollout of security controls. To further the cause of cybersecurity in healthcare, Kate actively collaborates with the HSCC CWG and the 405(d) program, and consistently advocates at the federal and state levels to fortify cybersecurity within healthcare organizations.

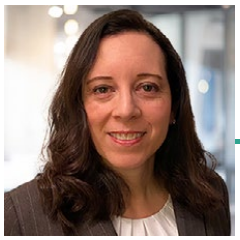
**TIM (T.J.) RAMSEY**
*Senior Director, Threat Assessment Operations*
Fortified Health Security

T.J. Ramsey is a seasoned IT security professional with 18 years of experience focused on healthcare and defense intelligence. He served as a U.S. Army Military Intelligence Analyst for the Department of Defense, and held security roles at Obsidian Solutions Group and SAIC/Leidos. T.J. has shared his cybersecurity expertise in publications like *TechTarget* and *Chief Healthcare Executive* and presented at industry events, including Health Connect Partners (HCP), CHIME, and THIMA.



**MARK GILBERT**
*Manager of Digital Forensics & Incident Response*
Fortified Health Security

Mark Gilbert's impressive career includes 13 years as a Special Agent with the Department of Homeland Security, where he specialized in electronic crimes, digital forensics, network intrusion, and SCADA assessments for protective venues. Mark's dedication to public service also includes serving in the Naval Reserves, and as a Police Officer and State Trooper in North Carolina. Following his law enforcement career, Mark transitioned to the private sector, focusing on IT security, consulting in fraud detection, and developing customized software for various security controls.



**TAMRA DURFEE**
*Virtual Information Security Officer*
Fortified Health Security

Tamra Durfee is an experienced CISO with over 25 years in information security, compliance, regulatory risk, strategy, innovation, and technology transformation. For the past 8 years, she has specialized in healthcare cybersecurity and building risk-based medical device information security programs. She is a presenter at HIMSS, CHIME, CHA, and a healthcare security contributor to *Healthcare IT News*. Tamra holds certifications as a Certified Healthcare CIO (CHCIO), Certified Digital Healthcare Executive (CDH-E), GIAC Security Leadership Certification, Certified Professional in Healthcare Information Management Systems (CPHIMS), and IBM Certified Solutions Architect.

**JAKE BICE**
*Director of Cybersecurity Operations*
Fortified Health Security

Jake Bice 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.


## Enjoyed reading this report?

Explore additional content on our website where you'll discover current and past issues of our Horizon Reports, engaging blogs authored by healthcare cybersecurity experts, access on-demand and live webinars, and a trove of other valuable resources.

Join us on a journey of continuous learning and discovery:

www.fortifiedhealthsecurity.com


Healthcare's Cybersecurity Partner®

# About Fortified Health Security

Fortified is Healthcare's Cybersecurity Partner® – protecting patient data and reducing 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.

Fortified℠
HEALTH SECURITY

**www.fortifiedhealthsecurity.com**

connect@fortifiedhealthsecurity.com

2550 Meridian Blvd, Suite 190
Franklin, TN 37067