Fortified HEALTH SECURITY℠

2024 MID-YEAR HORIZON REPORT

The state of cybersecurity in healthcare

About the Horizon Report

Fortified Health Security's Horizon Reports are 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 landscape 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 reach this year's midpoint, we've already witnessed incidents and legislative progress that will likely influence healthcare cybersecurity for years to come. These developments shape the focus of our mid-year report, continuing our tradition of providing timely insights and guiding proactive strategies.

The headlining cybersecurity stories so far this year are the cyber attacks on Change Healthcare and Ascension, both of which caused massive disruption throughout the entire healthcare ecosystem.

These unparalleled incidents serve as a stark reminder of the vulnerabilities faced by healthcare organizations, particularly concerning third-party vendors throughout the entire healthcare supply chain and the rise in more sophisticated social engineering attacks.

It also emphasizes the importance of business continuity planning and the need to have robust plans in place to ensure the uninterrupted delivery of healthcare services, no matter the scale of disruption.

Encouragingly, there has been notable progress on the legislative front. The increasing support from policymakers, including how to provide more funding, the release of the Cybersecurity Performance Goals (CPGs) by HHS, in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), and the elevated awareness around the severe threats facing our industry mark significant steps forward.

However, there remains much work to be done, especially in the area of access controls. Many organizations still need to adopt more comprehensive security measures to adequately protect themselves and their patients.

As we continue to address these challenges, your active engagement and collaboration are crucial to advancing our shared goals in healthcare security. Your commitment to this partnership not only enhances our collective strength but also sets the foundation for lasting success.

Thank you for your trust, partnership, and dedication as we move forward together.

Warm regards,

Dan L. Dodson

2024 Mid-Year in Review

The data reported to the U.S. Department of Health and Human Services Office for Civil Rights (OCR) from January 1 to June 30, 2024, paints a rosy picture: fewer patient records exposed than last year.

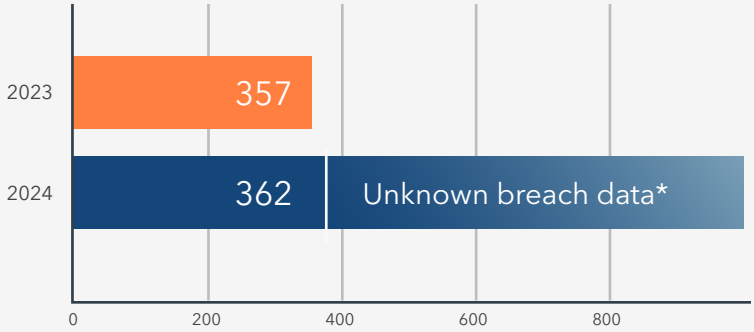
But this apparent calm conceals deeper chaos. The absence of breach reports related to Change Healthcare and Ascension means that crucial details around the impact of cyber attacks on healthcare are missing.

Once these breaches are officially reported, the true and alarming reality will come into stark focus.

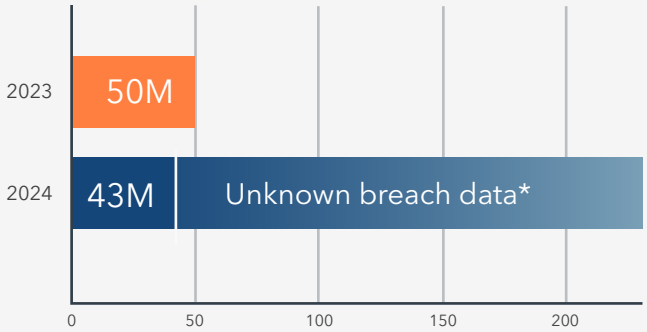
Number of breaches and patient records exposed

Considering Change Healthcare's reach—touching 1 in every 3 patient records nationwide—the OCR's breach data for 2024 only scratches the surface. The real numbers of breaches and exposed patient records are likely higher than what's currently reported.

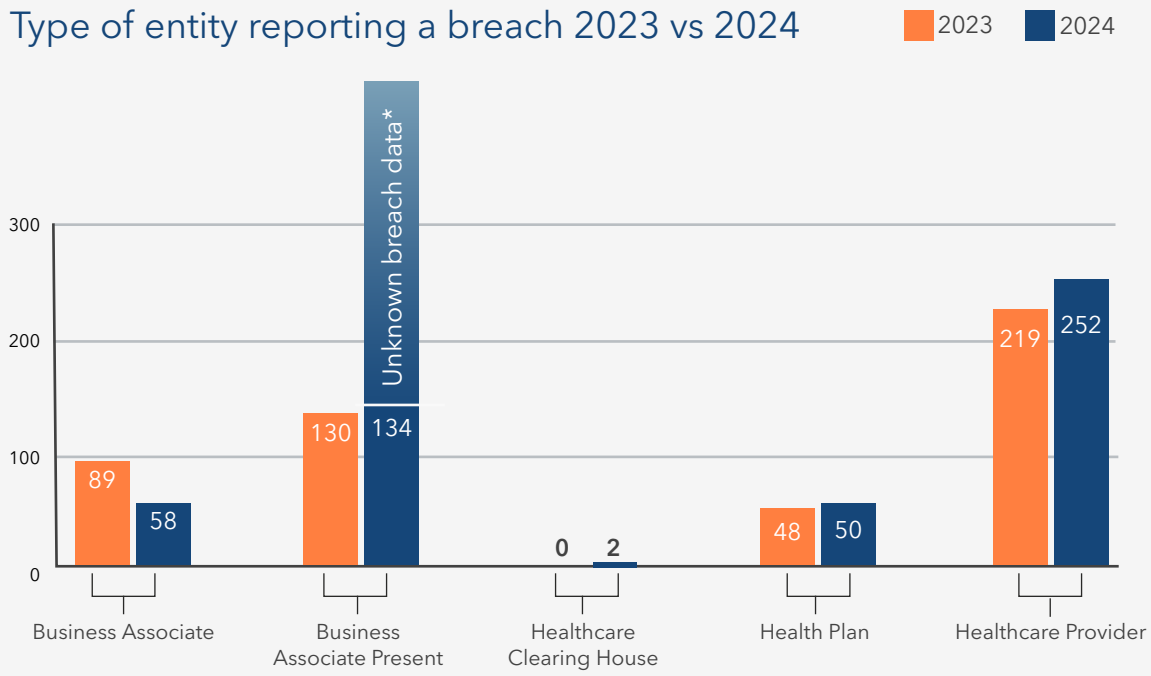
Breaches mid-year
2023 vs 2024



Patient records exposed mid-year
2023 vs 2024



*At time of print, Change Healthcare and Ascension breach data has not been reported to the OCR so actual numbers are unknown.



*At time of print, Change Healthcare and Ascension breach data has not been reported to the OCR so actual numbers are unknown.

Despite the number of breaches reported by Business Associates (BAs) decreasing by 35% year-over-year (YoY), BA-related breaches still account for almost 39% of all reported breaches. This underscores the ongoing importance of robust third-party risk management in healthcare cybersecurity.

Another notable mid-year change to monitor is the reported breach data for BA Present and Healthcare Providers. It's currently unclear whether Change Healthcare will report these breaches or if individual providers will need to submit their data to the OCR. If individual reporting is required, we anticipate a significant increase in mid-2024 breach data for both of these entities.

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

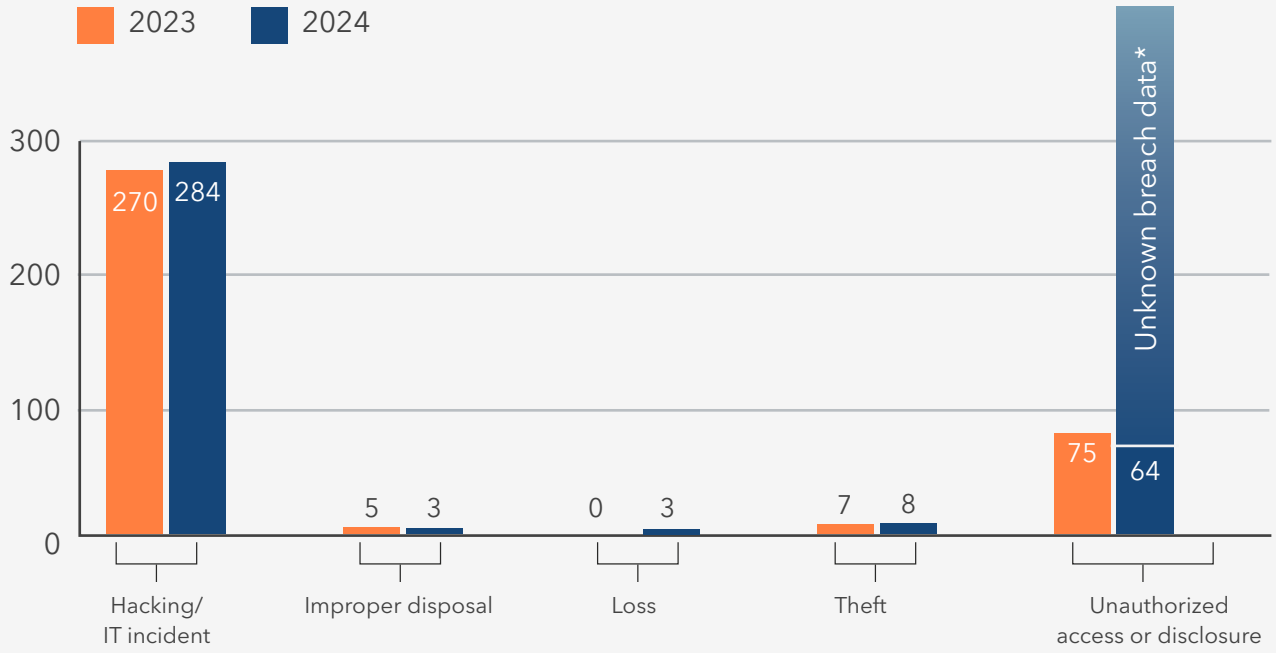
Entity that assumes the risk of paying for medical treatments. E.g., uninsured patient, self-insured employer, payer, or Health Maintenance Organization (HMO).

Healthcare Provider

A person trained and licensed to give health care; a place licensed to give health care. E.g., doctors, nurses, and hospitals.

Type of breaches mid-year 2023 vs 2024

While mid-year OCR data shows breach tactics either declining or remaining flat YoY, the full impact is yet to be seen. These figures are expected to increase once the breach data from Change Healthcare and Ascension is disclosed to the OCR. This is particularly true for incidents of unauthorized access or disclosure, especially if individual providers are responsible for reporting how their data was accessed.



*At time of print, Change Healthcare and Ascension breach data has not been reported to the OCR so actual numbers are unknown.

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.

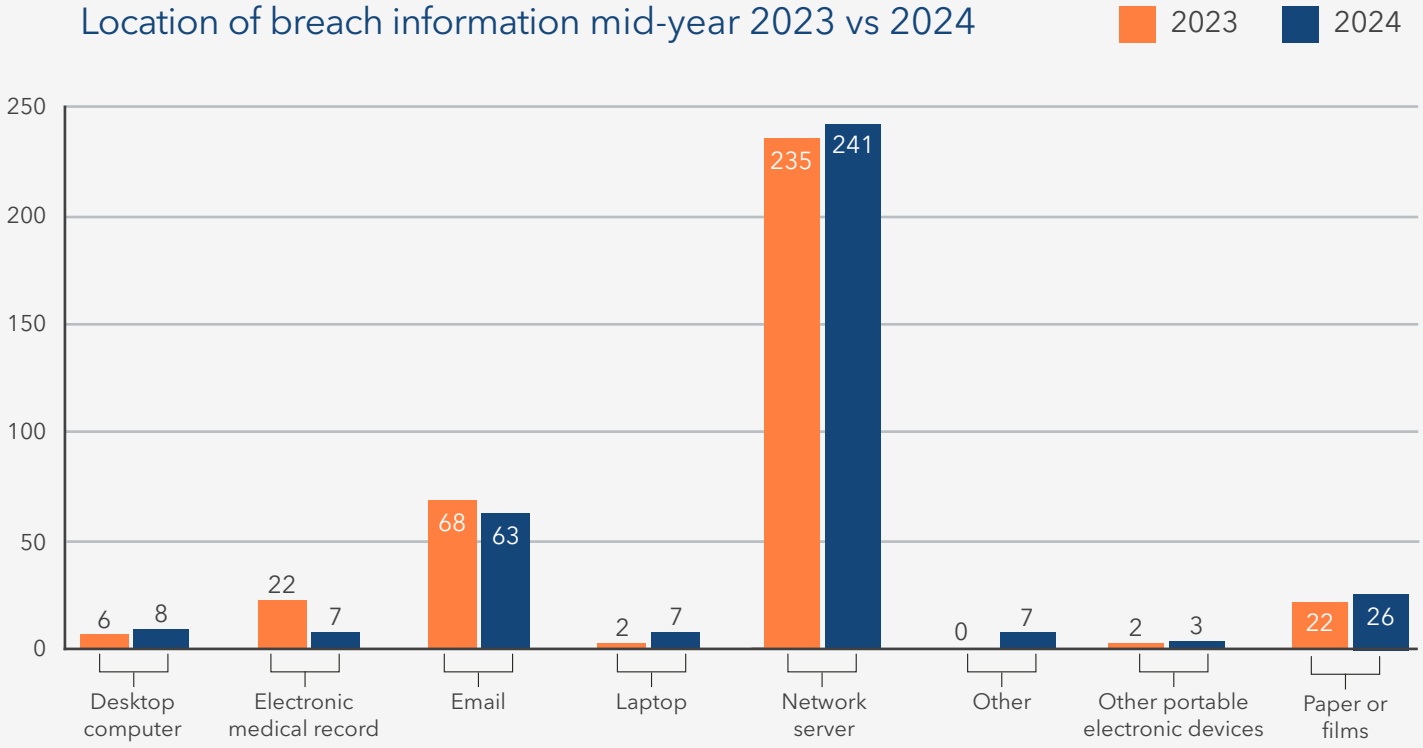
Unauthorized Access/Disclosure

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

Network servers remain the primary focus for threat actors targeting healthcare organizations. These servers often house the most sensitive patient data and are interconnected with critical systems, making them prime targets. By fortifying these defenses, especially through stronger vulnerability threat management, healthcare organizations will be better equipped to prevent breaches and safeguard patient information.

Location of breach information mid-year 2023 vs 2024



About this data

This report is based on data collected from OCR's databases and public records, covering the periods from January 1, 2024, to June 30, 2024, and from January 1, 2023, to June 30, 2023, for comparative purposes. 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.

Synchronize for stronger healthcare security

Mid-year OCR data shows that risks to healthcare organizations, patient health information, and patient care are still prevalent.

Recent trends involving third parties and Business Associates indicate a need for healthcare organizations to better synchronize their business, operational, and cybersecurity teams.

By consolidating efforts, enhancing strategic planning, and improving communication, cybersecurity programs can evolve, thereby supporting the overarching goal of uninterrupted patient care.

The Legislative Landscape: Mid-Year 2024

The first half of 2024 was a busy time for legislative action regarding healthcare cybersecurity. While progress may seem slow, the speed at which the government is moving to address cybersecurity issues within our sector is unprecedented.

Since the release of the Health and Human Services (HHS) cybersecurity concept paper in December 2023, the momentum to address the risks that healthcare systems face has continued well into the first half of 2024. Below is a recap of the most significant developments.

HHS Cybersecurity Performance Goals

In January, HHS kicked off the new year by introducing the Health and Public Health (HPH) Cybersecurity Performance Goals (CPGs), which include 10 Essential and 10 Enhanced goals for healthcare organizations. They are mapped to both the Health Industry Cybersecurity Practices (HICP) and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

HHS developed these goals in collaboration with executives from the Health Sector Coordinating Council Cybersecurity Working Group (HSCC CWG).

If you haven't had a chance to review these goals, now is the time so that you're prepared for when they move from voluntary to required.

Essential Goals

These goals are aimed at helping healthcare organizations address common vulnerabilities by setting safeguards that will better protect them from cyberattacks, improve response when events occur, and minimize residual risk.

They are designed to be achievable by all healthcare organizations and center around:

- Mitigating known vulnerabilities
- Email security
- Multi-factor authentication
- Basic cybersecurity training
- Strong encryption
- Revoking credentials for departing workforce members, including employees, contractors, affiliates, and volunteers
- Basic incident planning and preparedness
- Unique credentials
- Separate user and privileged accounts
- Vendor and supplier cybersecurity

Enhanced Goals

These goals are designed to help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors. They address:

- Asset inventory
- Third-party vulnerability disclosures
- Third-party incident reporting
- Cybersecurity testing
- Cybersecurity mitigation
- Detecting and responding to relevant threats and tactics, techniques, and procedures (TTP)
- Network segmentation
- Centralized log collection
- Centralized incident planning and preparedness
- Configuration management

Health and public health cybersecurity gateway

In conjunction with the release of the CPGs, HHS also announced the creation of a new "one-stop" website for cybersecurity information and resources. These resources include best practices, guidance, education, threat intelligence, and other cybersecurity information specifically for healthcare.

Be sure to bookmark https://hphcyber.hhs.gov/ to stay abreast of all the movement currently underway across the sector.

HSCC's 5-year strategic plan

In February, the Health Sector Coordinating Council Cybersecurity Working Group (HSCC CWG) announced its five-year strategic plan to move healthcare from a critical state to a stable state by 2029.

The plan is a culmination of 18 months of hard work. It presents seven major industry trends expected over the next five years, as well as a strategy to increase the cyber resilience of the industry.

The plan details 10 cybersecurity goals for a resilient sector and outlines 12 objectives to assist with meeting those goals. The full plan can be found on the HSCC website.

Five-Year Cybersecurity Goals to Address Industry Trends

Health Sector Coordinating Council Cybersecurity Working Group

G1	Healthcare and wellness delivery services are user - friendly, accessible, safe, secure, and compliant	G6	Healthcare technology used inside and outside of the organizational boundaries is secure-by-design and secure-by-default while reducing the burden and cost on technology users to maintain an effective security posture
G2	Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners	G7	A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers, including non-traditional health and life science entities
G3	Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health subsectors	G8	Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing
G4	Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements	G9	The health and public health sector has established and implemented prepardness response and resilience strategies to enable uninterrupted access to healthcare technology and services
G5	Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use	G10	Organizations across the health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels within each organization

Source: HSCC

Five-Year Cybersecurity Objectives to Implement the Goals

Health Sector Coordinating Council Cybersecurity Working Group

01	Develop, adopt and demand safety and resilience requirements for products and sercvices offered, from business to business, as well as health systems to patients, with the concept of secure-by-design and secure-by-default	07	Increase incentives, development and promotion of health care cybersecurity-focused education and certificate programs
02	Simplify access to resources and implementation approaches related to the adoption of controls aligned with regulatory and sector standards for securing devices, services, and data	08	Increase utilization of automation and emerging technologies like A.I. to drive efficiencies in cybersecurity processes
03	Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco-system	09	Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements
04	Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies	010	Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks
05	Emerging health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organization	011	Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness
06	Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organization (e.g., rural health)	012	Develop mechanisms to enable “mutual aid” support across sector stakeholders to allow for timely and effective response to cybersecurity incidents

Source: HSCC

Fortified had the distinct pleasure of participating in the formulation of this five-year plan and is committed to assisting in meeting the objectives and goals within the healthcare industry.

Visit our blog “Charting a Wellness Plan for Healthcare Cybersecurity” to keep an eye on this plan as it progresses.

> cybersecurity is not merely an IT function, but an **organization-wide strategy** to address enterprise risk management

NIST CSF 2.0

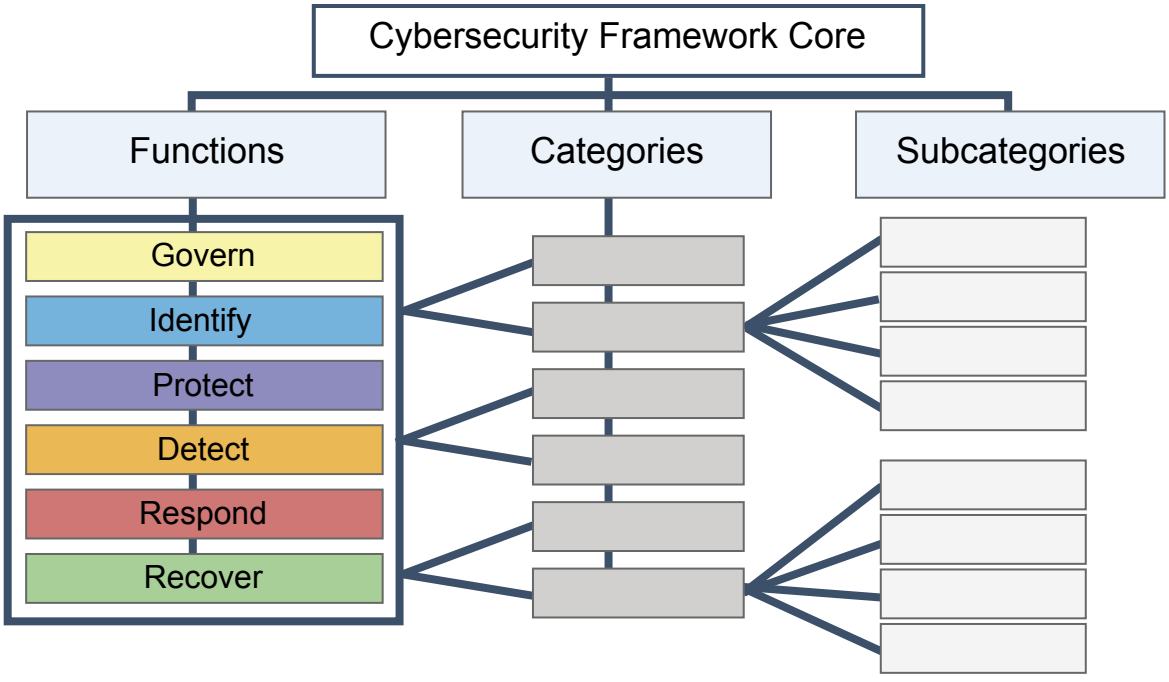
The same day HSCC announced its five-year plan, NIST released its updated Cyber Security Framework (NIST CSF 2.0).

NIST is the most frequently used cybersecurity standard in the industry – nearly 60% of healthcare organizations employ this framework. In fact, a recent study indicated that the application of NIST CSF and/or the Health Industry Cybersecurity Practices (HICP) resulted in lower cyber insurance premium growth.

Fortified highly recommends the adoption of either of these standards to grow your cybersecurity posture.

The newly released NIST CSF 2.0 standard has a number of changes intended to address the industry's current cyber attack environment. The most significant change is the inclusion of a sixth pillar, Govern, to complement the previous pillars: Identify, Protect, Detect, Respond, and Recover.

The Govern pillar addresses the need for organizations to have oversight of the other five functions, and prioritize outcomes based on the organizational mission and stakeholder expectations. This solidifies the fact that cybersecurity is not merely an IT function, but an organization-wide strategy to address enterprise risk management.



HHS releases proposed FY2025 budget

In March, HHS released its proposed FY2025 budget. Given it has been 28 years since the last budget passed congress, some healthcare cybersecurity funding allocations are included.

The proposal identifies $1.3B to assist under-resourced healthcare organizations in achieving the above-mentioned CPGs. The structure is similar to the previous Promoting Interoperability Program (PIP), which was the reporting basis for Meaningful Use.

$1.3B to assist under-resourced healthcare organizations

Funding would begin in FY '27-'28 with $800M designated to assist high-need hospitals in adopting the Essential CPGs, and continue with another $500M in FY '29-'30 to assist all hospitals with meeting the Enhanced CPGs, which is promising news.

The budget also includes proposed Centers for Medicare and Medicaid Services CMS reimbursement cuts for organizations that are not meeting the Essential CPGs beginning in FY '29.

Fortified will continue to monitor any developments that might assist our clients with furthering their cybersecurity posture, which will hopefully also include other future funding avenues.

CIRCIA proposed rulemaking

The long-awaited Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) finally entered into proposed rulemaking on April 4th, with a 60-day comment period. The legislation was created in response to the 2022 Act calling for Cybersecurity and Infrastructure Security Agency (CISA) to implement statutes on the reporting of cyber incidents and ransomware payments.

This proposal attempts to clarify what rule would be enacted in a particular circumstance, such as a:

- Cyber Incident
- Covered Cyber Incident
- Substantial Cyber Incident

CISA proposes that only Substantial Cyber Incidents by Covered Entities would be affected by the rule. The timeline for the full implementation of CIRCIA is currently projected for September 2025.

For further clarification, see the Harmonization of Cyber Incident Reporting to the Federal Government.

Government reaction to the Change Healthcare incident

Based on the multiple congressional hearings in the spring of 2024, the Change Healthcare cyber attack has the full attention of congress, HHS, and other government agencies. This attack revealed the cracks in our national healthcare infrastructure and the urgent need to fill some of the gaps.

Following the attack, the response from the HHS was relatively slow, largely because the agency initially underestimated the extensive impact that the incident would have across the healthcare sector.

While early reports focused on the impact to pharmacy operations, in the weeks that followed it became clear that this attack created significant challenges to many key operational areas in the majority of healthcare systems.

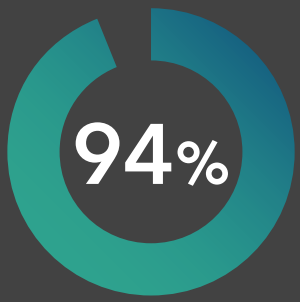
In fact, a survey by the American Hospital Association showed that 74% of hospitals had direct patient care impact, and 94% of hospitals reported a financial impact.

On April 16th, the Energy & Commerce Health Subcommittee held a hearing titled "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack" to consider expert testimony concerning the attack, and discuss how the government could aid in recovery and prevent similar incidents in the future.

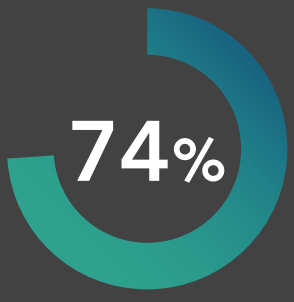
Subsequently, on May 1st, Andrew Witty, CEO of UnitedHealth Group (UHG), appeared before two congressional committees to discuss the Change Healthcare breach. Following the hearing, Senator Ron Wyden (D-OR), sent a letter to HHS calling on the department to institute a number of changes, including:

- Requiring minimum, mandatory cybersecurity standards for systemically important entities (SIEs)
- Regular auditing of health organizations
- Support following a breach to ensure rapid recovery
- Technical assistance to hospitals and other health providers

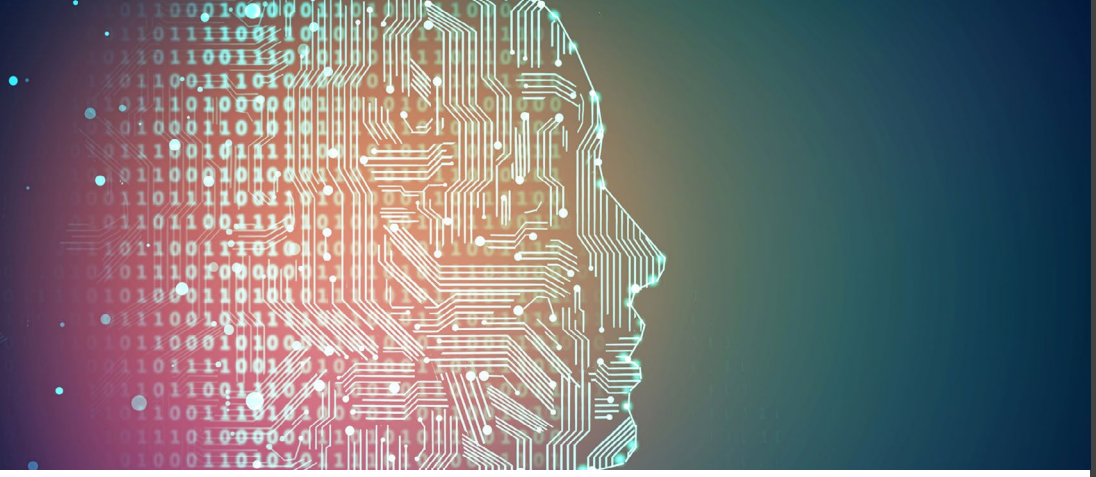
A full recording and access to the written testimony of the panelists is on the subcommittee website. A recap of this hearing can be found on our blog.



hospitals reported a financial impact



of hospitals had direct patient care impact



An update to the EO on AI

As we shared in our 2024 Horizon Report, President Biden issued an EO to address challenges with AI and ensure its use is safe and secure in October 2023.

According to a March 28th update, all of the 150-day actions tasked in the EO were completed.

By December 1st, 2024, federal agencies will be required to implement concrete safeguards when using AI to ensure that, "When AI is used in the Federal healthcare system to support critical diagnostics decisions, a human being is overseeing the process to verify the tools' results and avoids disparities in healthcare access."

The most notable contributions in early 2024 include the Department of Homeland Security's release of an "Artificial Intelligence Roadmap 2024," which outlines three focal areas:

- Responsibly leverage AI to advance homeland security missions
- Promote nationwide AI safety and security
- Continue to lead in AI through strong, cohesive partnerships

In addition, CISA released "Safety and Security Guidelines for Critical Infrastructure Owners and Operators" in response to the EO, outlining both the opportunities and the risks of AI. All critical infrastructure sectors were encouraged to leverage the NIST "AI Risk Management Framework (RMF)" to assist with managing the use of AI within their environment.

Executive order to protect sensitive data

On February 28th, President Biden signed the executive order (EO) "Preventing Access to American's Bulk Sensitive Data and the United States Government-Related Data by Countries of Concern."

The White House considers this the "most significant executive action any President has ever taken to protect Americans' data security."

This EO seeks to:

- Create prohibitions and restrictions on certain data transactions
- Focus on "countries of concern"
- Increase attention on network infrastructure
- Define six categories of sensitive personal data
- Increase focus on AI
- Emphasize new proposed restrictions on healthcare data

Proposed Health Care Cybersecurity Improvement Act of 2024

In late March 2024, Senator Warner (D-VA) introduced the Health Care Cybersecurity Improvement Act of 2024. This bill aims to set minimum cybersecurity standards that entities must meet to qualify for Medicare accelerated and advance payments in the event of a cybersecurity incident.

Specifically, the legislation targets amendments to the Medicare Hospital Accelerated Payment Program and the Medicare Part B Advance Payment Program. If passed, this measure would significantly impact organizations facing cyber incidents, as it would condition access to advance funding on compliance with these new standards. By linking financial assistance to cybersecurity compliance, particularly adherence to the HHS CPGs, the bill intends to incentivize organizations to enhance their cybersecurity posture.

Critical infrastructure memo

On April 30th, 2024, the White House released a pivotal National Security Memorandum on Critical Infrastructure Security and Resilience.

This directive:

- Emphasizes the urgent need to safeguard vital systems from a range of evolving threats such as cyber attacks, physical disruptions, and natural disasters
- Outlines a robust framework to strengthen the security and resilience of key sectors
- Clarifies U.S. policy principles and objectives
- Assigns specific roles and responsibilities to stakeholders
- Promotes a unified risk-based approach to effectively reduce vulnerabilities

Cybersecurity support for rural hospitals

On June 10th, Microsoft and Google announced a collaboration with the American Hospital Association and the National Rural Health Association to help rural hospitals enhance their cybersecurity defenses.

Microsoft plans to:

- Offer nonprofit pricing to Critical Access and Rural Emergency Hospitals
- Provide a year of free advanced security tools to larger rural hospitals
- Extend Windows 10 security updates for an additional year at no cost
- Offer free cybersecurity assessments and training through their partners

Google plans to:

- Provide advice on endpoint security
- Offer discounts on communication tools and security support
- Fund software migration
- Start a pilot program with rural hospitals to develop security solutions tailored to their specific needs

These initiatives from Microsoft and Google are still in the planning stages and are designed to last for one year. Given their limited duration, it's crucial for organizations to meticulously evaluate these solutions. This includes thoroughly assessing recommended security enhancements and ensuring that staff training is aligned with their needs.

Due to their temporary nature, rural hospitals in particular should carefully consider if these short-term programs are compatible with their long-term cybersecurity strategies, or if more permanent, sustainable solutions are required.

Looking ahead

The government's heightened attention on cybersecurity in healthcare is unprecedented, highlighting the serious threats to our critical infrastructure.

As we navigate through 2024, staying updated on federal actions is not just advisable—it's essential. Upcoming regulations, refined AI protocols, and possible incentives are on the horizon.

With highly orchestrated and extremely sophisticated attacks happening at scale, these developments signal key areas for strategic planning and proactive engagement to safeguard our healthcare.

The Imperative for Business Continuity in Healthcare

When unexpected disruptions happen in a healthcare environment, they can pose significant challenges to patient care, operations, and overall organizational stability. As security threats to healthcare continue to evolve, organizations must embrace a dynamic approach to business and cybersecurity resiliency through robust business continuity planning.

In healthcare, business continuity planning involves strategic and proactive efforts to ensure the uninterrupted delivery of patient care and critical services while also maintaining operational integrity during disruptions.

These events can range from natural disasters and pandemics to technological failures and cyber attacks like ransomware that might threaten normal operations. Recent examples include the cyber attacks on Change Healthcare and Ascension.

Lessons learned from Change Healthcare

Healthcare organizations worldwide can glean pivotal business continuity lessons from the Change Healthcare incident.

The importance of having basic and essential security measures in place, like multi-factor authentication (MFA), was underscored in the congressional testimony given by UnitedHealth Group's CEO, Andrew Witty on May 1st, 2024, regarding the Change Healthcare breach.

In his statements, Mr. Witty acknowledged the disruption that the breach caused the healthcare sector, providing detailed insights into the attack's origins, UnitedHealth Group's response to the event, and what they've learned in the aftermath of the attack.

Here are some takeaways from the Change Healthcare incident as they relate to business continuity planning:

1. Response to cyber attacks must be **swift, premeditated, and repeatable**
2. Enhancing healthcare resilience is now an **unquestionable priority**
3. Improvements in healthcare cybersecurity protections are **mandatory**
4. Prioritizing detailed business impact analysis across healthcare departments is essential to **understanding operational impacts and downtime**

Where business continuity adds value in healthcare

A well-crafted business continuity plan (BCP) supports healthcare organizations in five key areas, enabling them to swiftly adapt and protect patient care while ensuring uninterrupted service delivery:

01. Financial stability

Business disruptions, such as having your medical billing system disconnected or insurance claims processing delayed, can lead to financial losses and severe operational inefficiencies.

BCPs not only address immediate patient care concerns but also provide a roadmap for navigating financial challenges, ensuring that the organization remains financially resilient.

02. Regulatory compliance and legal protection

In highly regulated industries such as healthcare, compliance with various standards (e.g., HIPAA, OSHA, etc.) is paramount. Healthcare organizations often strive to exceed regulatory minimum requirements to enhance patient safety, improve quality of care, and safeguard sensitive information.

Through annual risk analysis and continuous incident response engagements (e.g. monthly fire drills and quarterly tabletop exercises), healthcare organizations can proactively mitigate identified risk, ensure rapid and measured response to incidents, and exceed minimum regulatory requirements.

Business continuity planning requires an organization to thoroughly understand the implications should a critical service or process become unavailable. To analyze the impact, it's essential to establish clear downtime procedures and recovery strategies for restoring these functions within agreed-upon timelines. This systematic approach ensures minimal disruption, swift recovery, and sustained operational resilience.

In addition to helping shield healthcare organizations from other impacts like legal consequences, BCPs can also help maintain the organization's reputation as a trusted and reliable provider within their local community.

03. Emergency preparedness and response

An effective BCP should encompass comprehensive emergency preparedness and incident response (IR) strategies.

For example, if there's a sudden surge in patient volume or the need for rapid deployment of resources, the BCP should outline clear communication channels, and define roles and responsibilities to ensure the healthcare organization can respond effectively and efficiently.

An ineffective or untested BCP can significantly extend response and recovery times, adversely affecting service delivery and overall business resilience. The duration of recovery following an incident is directly proportional to the quality and maturity of the BCP in place.

> An ineffective or untested BCP can **significantly extend** response and recovery times

04. Supply chain resilience

The healthcare industry heavily relies on a complex and interconnected supply chain for medications, medical supplies, and equipment. If these supply chains are disrupted, it can have cascading effects on patient care.

For example, interruptions in the production of critical drugs, such as antibiotics, chemotherapy agents, or insulin, can lead to delays or rationing of treatment for patients with infectious diseases, cancer, or diabetes.

The Change Healthcare incident elevated the urgency around business resiliency and reliance on third-party service providers. The abrupt and unforeseen cessation of payment processing triggered unprecedented disruptions, severely impacting the entire healthcare sector.

Overall, disruptions in the healthcare supply chain can have serious implications for patient care, highlighting the need for proactive risk management, contingency planning, and collaboration among stakeholders to ensure the resilience and reliability of healthcare supply chains.

05. Telemedicine readiness

Telemedicine is on the rise in healthcare, allowing organizations to remotely provide consultations and monitor patients. Integrating telemedicine into BCPs equips healthcare organizations to adapt to disruptions caused by unforeseen challenges or crises more effectively.

The strategic imperative of business continuity planning

Healthcare organizations that prioritize business continuity planning are more adept at managing situations that could compromise patient care, financial stability, regulatory compliance, and overall operational availability and integrity.

Proactively investing in business continuity and resilience strategies will yield substantial benefits when they are most needed.

Access Controls: Moving Beyond Security Best Practices

Too many hospitals and health systems across the country implement "best practices" that are not enough to safeguard against cyber attacks.

Breaches to healthcare organizations stemming from "unauthorized access or disclosure" soared 133% from 2022 to 2023. Many of these organizations aren't negligent; their security measures simply don't go far enough.

To fortify your cybersecurity posture beyond the foundational level, we've identified four critical areas of access control that can significantly lower your healthcare organizations' risk exposure while strengthening your defenses against potential cyber attacks.

01. Universal MFA

Over 60% of data compromises in the first quarter of 2023 were the result of credential issues. By requiring a second verification method along with a password, such as an app-generated code or fingerprint scan, multi-factor authentication (MFA) acts as the intimidating guardian at the gate.

However, the real challenge lies not in the absence of MFA, but in its deployment.

Having only partial access control security is like using an umbrella with holes. When the bad weather hits, it won't matter if most of the umbrella is fine. One hole will be enough for you to understand what insufficient protection feels like.

The solution

Universal implementation of MFA, including:

- Normal and privileged users
- Cloud and on-premise applications
- Vendor accounts
- Server and workstation access
- All public-facing assets, including remote access VPNs

02. Passwords

Successful credential attacks often stem from a single issue: predictable password habits.

In the midst of our time-pressed morning scramble, logging into a deluge of applications is common practice. To expedite this process, many fall into the routine of recycling passwords. However, if one is breached, it's open season on multiple accounts.

Ransomware groups love exploiting patterns, like the ever-popular password "Summer2023!" And when it's time to update those passwords, users too often make minimal changes, such as swapping a number or tweaking the last character. Unfortunately, these variations are often easy to guess.

And another issue? Storing passwords in a file labeled "passwords.txt." That's akin to leaving your house keys under the mat.

The solution

- Lean on password managers to create and store complex passwords
- Prohibit the storage of passwords in unsecure locations
- Implement comprehensive password policies that check for complexity, history, and validation against well-known common passwords

03. Domain Admins

A domain admin account is the most coveted account a hacker can access. It gives them extensive power over an entire network, including the ability to manipulate accounts and access sensitive data. However, securing domain admin accounts requires more than crafting a long, complex password.

A strategy that can make or break your organizations' security is the principle of least privilege—the practice of granting users only the essential access needed for their roles.

To apply this "best practice," many organizations separate "normal user" accounts from "administrators," thinking they're safe as long as the majority of users are in the "normal" category.

Unfortunately, this oversight excludes three essential areas of least privilege:

1. Minimizing the scope of domain admin account
2. Locking down high-impact tools
3. Administrators who don't need access to all assets and all elevated privileges

To throw a wrench in a hacker's plans, restrict the number of machines a domain admin logs into, and disable cached credentials. These actions will prevent passwords from being saved to these systems.

Service accounts

Administrators sometimes add service operation accounts as domain admins. This increases the security risk to the organization, particularly if the passwords associated with these accounts are rarely, or never, changed.

With just one successful phishing attempt, an attacker could log in and extract these outdated passwords from the computer's memory, thereby gaining the same access privileges as a domain admin.

The solution

- Limit domain admin group membership to what's strictly necessary
- Ensure privileged accounts have access only to critical systems
- Mandate that admins use standard accounts for day-to-day operations
- Don't allow service accounts to "interactively logon." Service accounts are intended for use by applications or services, not users, and usually have higher privileges than end-user accounts.

Remote access applications

The principle of least privilege also applies to applications, especially those with remote access features. These tools are prime targets for hackers because they blend in with normal network traffic.

The top five reported ransomware groups in 2023—Lockbit, BlackCat, CL0P, Black Basta, and Play ransomware—used non-default remote desktop applications in their attacks, like TeamViewer, AnyDesk, PsExec, or ScreenConnect.

Similarly, ransomware attacks often exploit built-in command tools like PowerShell and command prompt.

The solution

- Restrict these tools to IT staff
- Require MFA for external access
- Limit file types that employees can download

> phishing attackers have found ways around **MFA in Outlook**

04. Email

In 2023, phishing emails were responsible for one-third of all data breaches. This trend is underscored by recent incidents such as Black Basta's attack on Ascension. This group frequently uses phishing to gain initial access to networks.

Although the use of AI is making the telltale signs of a phishing email harder to spot, there are effective methods for automating the process of blocking unauthorized email access.

Certain tactics may seem redundant with MFA set up; however, phishing attackers have found ways around MFA in Outlook. Two methods in particular are worth noting:

1. Exploiting legacy authentication

Older email protocols that don't accommodate MFA provide an opportunity for attackers to force a log on using legacy authentication (e.g., only a correct password).

Microsoft reports that over 97% of credential stuffing and 99% of password spray attacks attempt to exploit legacy authentication. By proactively disabling basic authentication, you can mitigate this risk.

2. MFA bombing

This emerging threat tactic floods an MFA app with login notifications in the hopes that a user will accidentally approve an unauthorized attempt out of frustration.

The solution

Geoblocking. Tool automation has made launching password brute force attacks relatively easy, with attempts originating from all corners of the globe. By blocking logins from countries not on your allow list—i.e., geoblocking—you can set rules that mitigate these threats and unauthorized access attempts following a phishing email.

The high cost of average access controls

Healthcare data breaches are not only disruptive, damaging, and stressful, they are also expensive, averaging almost $11 million per incident.

In the face of rising costs and persistent threats, the healthcare industry must reevaluate how it's protecting organizations and patient data.

However, implementing these steps to their fullest potential doesn't come without challenges for healthcare organizations. Short-term costs often take precedence over proactively avoiding future expenses, and employees may resist change to processes that they're familiar with.

Although these obstacles are important to recognize, the reality is that the financial repercussions, coupled with the cascading fallout from large breaches like Change Healthcare and Ascension, serve as a stark wake up call to leave no stone unturned with your defense strategy.

Vendor Dependency Risks:Lessons from the CrowdStrike Outage

In an interconnected world where IT and humans interact, understanding the ripple effect of technology failures is crucial. In the words of Barry Commoner, “Everything is connected to everything else."

On Friday morning, July 19th, 2024, a routine content update at CrowdStrike caused global operational issues for businesses. This incident highlights how one event can trigger a chain reaction affecting various operations and third-party services.

While technology aims to enhance efficiency, human error remains a factor. Therefore, leaders must not only have downtime procedures in place but also ensure they are well-documented, regularly tested, and supported by consistent staff training to maintain continuity of critical services, especially during tech outages.

The McAfee incident of 2010

This isn't the first major disruption caused by a cybersecurity vendor. In April 2010, McAfee's faulty antivirus update (DAT 5958) misidentified a critical Windows file (svchost.exe) as a virus, causing countless machines to crash or reboot continuously. This incident highlights the risks of single vendor dependency and led to widespread criticism and a reevaluation of vendor risk management practices.

The Change Healthcare hack

The CrowdStrike outage mirrors the severe ransomware attack on Change Healthcare in February 2024. Led by the ALPHV/BlackCat group, the attack caused massive disruptions to billing and care authorization portals, resulting in significant financial and operational impacts across the healthcare sector.

Risks of vendor dependency

These outages exemplify a growing concern in cybersecurity: trust. When even our trusted vendors can take us offline, who can we really trust? These incidents reveal the systemic risks businesses face when a single vendor's failure can impact millions. While security vendors offer effective, sophisticated, and comprehensive security solutions, their ubiquity can also become a single point of failure.

Balancing partnerships with in-house capabilities

While defense-in-depth strategies are effective for keeping bad actors out, they don't address disruptions caused by vendors. Tight budgets often lead healthcare organizations to bundle services as a cost-saving measure. However, when not managed properly, this approach can create single points of failure, increasing vulnerabilities to widespread disruptions.

The guardrails are tight, and security and IT teams are doing all they can to maintain course and navigate these complexities. To balance vendor partnerships with in-house capabilities, consider these four options:

01. Business continuity planning

Business continuity planning (BCP) entails creating strategies to ensure that critical business functions continue during and after a disruption. This includes identifying essential services and resources, establishing backup procedures, and preparing for various scenarios that could impact operations.

Organizations must also plan for scenarios where critical vendors experience failures by:

- Developing redundant systems and alternative solutions to maintain operations during an outage
- Conducting regular disaster recovery drills to ensure that all stakeholders know their roles and responsibilities during an incident
- Establishing clear communication protocols to inform employees, customers, and stakeholders during and after a disruption
- Regularly updating and testing these plans to adapt to new threats and ensure their effectiveness

> While security vendors offer effective, sophisticated, and comprehensive security solutions, their ubiquity can also become a **single point of failure**

02. Disaster recovery planning

Disaster recovery planning (DRP) focuses on restoring IT systems and data after a catastrophic event, such as a cyber attack, natural disaster, or hardware failure. To prepare your healthcare organization, it's essential to:

- Conduct a risk assessment to identify potential threats to IT systems, and assessing the likelihood and impact of each risk
- Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) to determine acceptable levels of data loss and downtime
- Implement backup solutions in secure, off-site locations, and testing these systems regularly to ensure quick and accurate data restoration

03. Third-party risk management

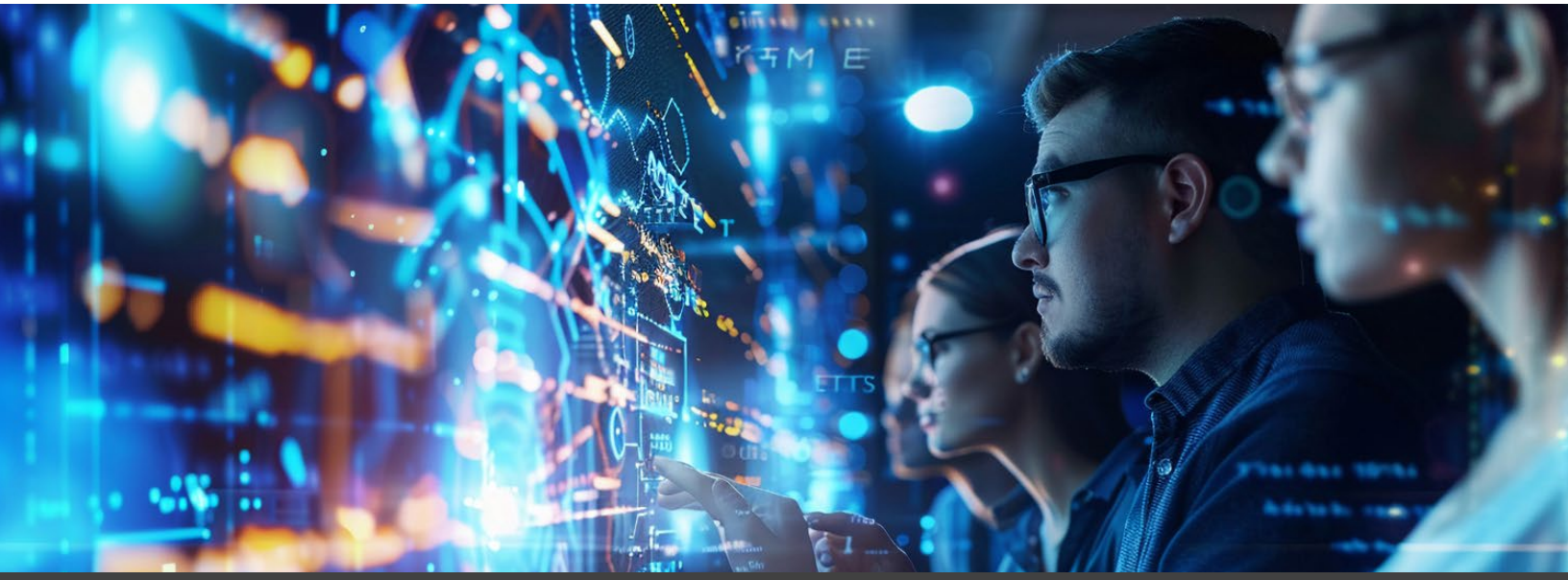
Third-party risk management (TPRM) involves assessing and mitigating risks associated with external vendors and service providers, including:

- Creating an inventory of all third-party vendors and classifying them based on the criticality of their services and the level of risk they pose
- Evaluating vendors' security practices, compliance status, and historical performance using standardized tools and questionnaires
- Implementing continuous monitoring of vendor performance
- Conducting regular audits of vendors to ensure adherence to security standards and contractual obligations

04. Tabletop exercises

Tabletop exercises (TTXs) simulate scenarios to help organizations practice responding to incidents like cyber attacks and operational disruptions. Key stakeholders collaborate to navigate the situation, identify weaknesses, and develop coordinated response strategies, improving overall preparedness. TTXs can involve:

- Identifying specific objectives and developing realistic scenarios that could impact the organization, focusing on potential disruptions most relevant to operations
- Gathering stakeholders from various departments, including IT, security, operations, and executive leadership, to provide comprehensive insights during the exercise
- Guiding participants through the scenario, prompting discussions on response strategies, and conducting a debrief to identify strengths, weaknesses, and areas for improvement



Embracing proactive strategies for cyber resilience

The CrowdStrike outage serves as a stark reminder of the complexities and risks associated with vendor dependency in cybersecurity. By adopting a balanced approach—leveraging multiple vendors, enhancing in-house capabilities, and implementing robust risk assessment and business continuity plans—organizations can better navigate these challenges. In an increasingly interconnected world, proactive risk management and strategic planning are essential business imperatives.

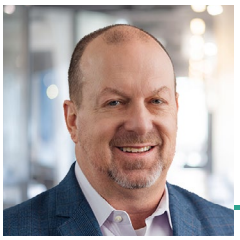
About the Contributors

DAN L. DODSON
Chief Executive Officer

As the CEO of Fortified Health Security, Dan 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

Throughout his distinguished career, William 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.

William is responsible for enhancing Fortified's services, delivery model, and security operations center, as well as streamlining operations among the sales, solution architect, account management, and customer success teams.

RUSSELL TEAGUE

Chief Information Security Officer

Russell is an innovative cybersecurity leader who shields healthcare organizations from digital threats. His experience spans three decades in information security, covering the Healthcare, Pharmaceutical, Financial, Retail, and Technology sectors.

A distinguished U.S. Army Intelligence veteran and leader, he's served as Chief Security Officer (CSO), Chief Technology Officer (CTO), and as a founder and board member for multiple leading cybersecurity companies. His sought-after cybersecurity expertise has led him to consult with the White House on the National Cybersecurity Healthcare Strategy, Health and Human Services (HHS), and participate with the Health Sector Coordination Council (HSCC).

Russell contributes his thought leadership to numerous publications and has presented at leading industry conferences, including CHIME, VIVE, MUSE, HIMSS, Healthcare IT Institute, Health Connect Partners, Oracle Health Conference, RSA, and Blackhat.

KATE PIERCE

Executive Director, Government Affairs

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.

ZOEY PRICKETT

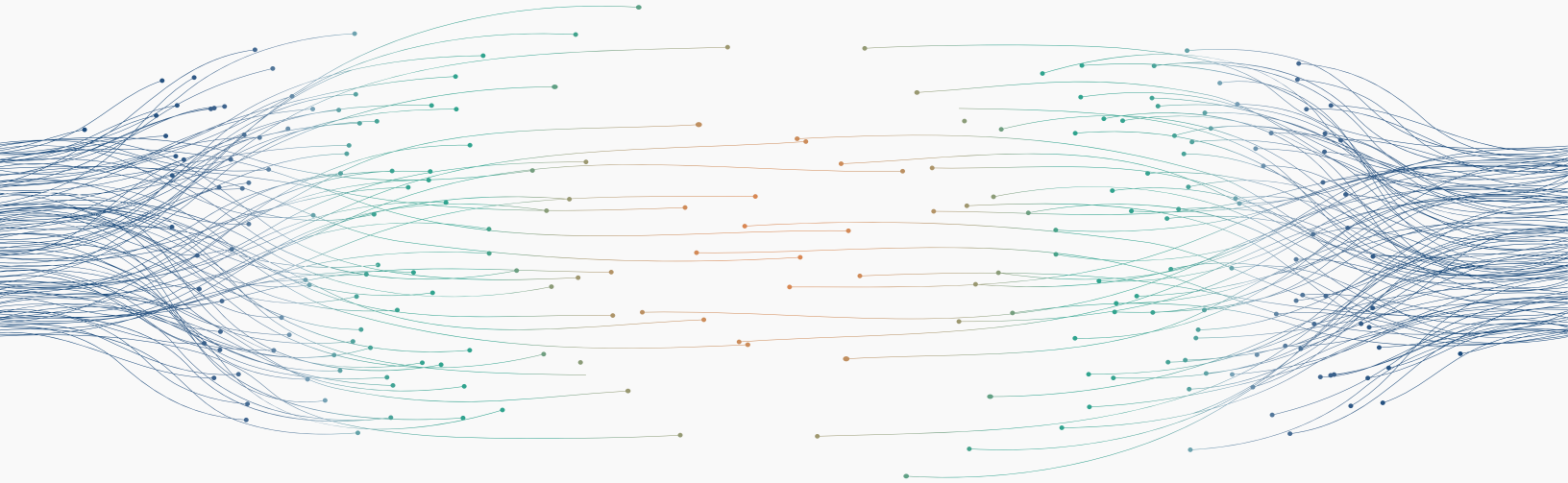
Senior Threat Analyst

Zoey Prickett is a Senior Threat Analyst with a strong focus on the healthcare sector, leveraging her IT background from BlueCross BlueShield of Tennessee. With a focus on defending networks from cyber threats, she contributes her expertise to assess and address possible security incidents, hunt for threats, and provide security or network configuration recommendations. By having a keen focus on proactive defense measures and continuous improvement, Zoey empowers healthcare organizations to stay ahead of cyber threats by helping improve the security and integrity of critical systems and data.

JAKE BICE

Director, Threat Defense Services

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.

Fortified HEALTH SECURITY℠

www.fortifiedhealthsecurity.com

connect@fortifiedhealthsecurity.com

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