Fortified HEALTH SECURITY

2023 Horizon Report

The state of cybersecurity in healthcare

CEO's message

Hospitals and health systems faced tremendous pressures, both internally and externally in 2022 not just from a cybersecurity perspective, but also in terms of profitability, expenses, and staffing. However, I remain optimistic that help is on the horizon. Healthcare organizations are struggling with the rigors of cybersecurity risk management and the impacts of breaches, and the problems are now escalating to the highest levels.

In November, Sen. Mark R. Warner, D-Va., published a policy paper, *Cybersecurity is Patient Safety*. In it, he details current cybersecurity threats facing healthcare providers and systems and offers up for discussion a series of policy proposals for improving cybersecurity across the industry. Warner is the chairman of the Senate Select Committee on Intelligence and has long advocated for greater attention to cybersecurity issues across industries, including healthcare-specific initiatives.[1]

"When it comes to cyberattacks affecting patient care, the question is no longer a matter of if or when, but how often and how catastrophic the consequences," the policy paper states.

Fortified Health Security prepared a detailed response to Sen. Warner's policy paper, which we hope will move the needle on government assistance to healthcare organizations and strengthen their security postures. We believe any initiative must:

- Allow flexibility to meet individual organizational needs
- Provide sustainable funding over time
- Include more post-risk assessment support
- Account for all elements required to reduce risk in both the short and long term

If lawmakers needed any more reminders about the importance of healthcare cybersecurity, they should look no further than the October breach of a large health system operating in 21 states, comprising 142 hospitals, and more than 2,200 care sites. The fallout still isn't known in terms of the number of breached records, but it's almost certainly significant.[2]

What the industry desperately needs is an infusion of money — now — to help cash-strapped hospitals and health systems move the needle on cybersecurity. What we don't need is another framework that takes years to formulate while attacks on hospital infrastructure, staff, and associated partners continue.

[1] Source: https://www.warner.senate.gov/public/index.cfm/2022/11/warner-releases-policy-options-paper-addressing-cybersecurity-in-the-health-care-sector
[2] Source: https://www.fiercehealthcare.com/health-tech/commonspirit-health-reported-it-security-incident-affecting-facilities-wash-neb-and
[3] Source: https://academynet.com/sites/default/files/q2_insights_briefing_2022_executive_summary_members.pdf

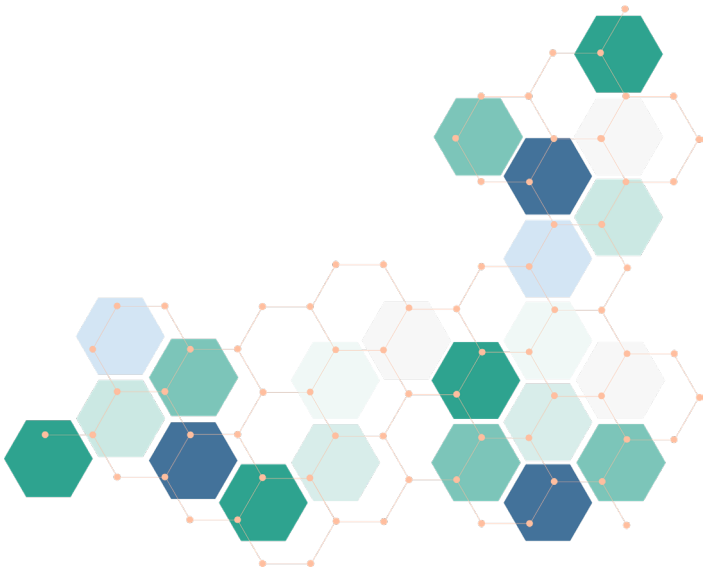
There is brighter news on the cyber front. A June financial outlook of leading health systems showed that 56% planned to "somewhat increase" cybersecurity spending, with another 31% saying that cyber spending would "significantly increase."[3] While more spending doesn't automatically equate to better security, it can when spent on the right things, which we detail throughout this report.

In addition to federal support for cybersecurity initiatives, hospitals will continue to mature the security postures of their organizations while also directing more attention and resources to manage the risks presented by third parties.

As you read the 2023 Horizon Report, we encourage you to share your security challenges and successes with us. We welcome your feedback and perspective at: horizonreport@fortifiedhealthsecurity.com.

Regards,

Dan L. Dodson



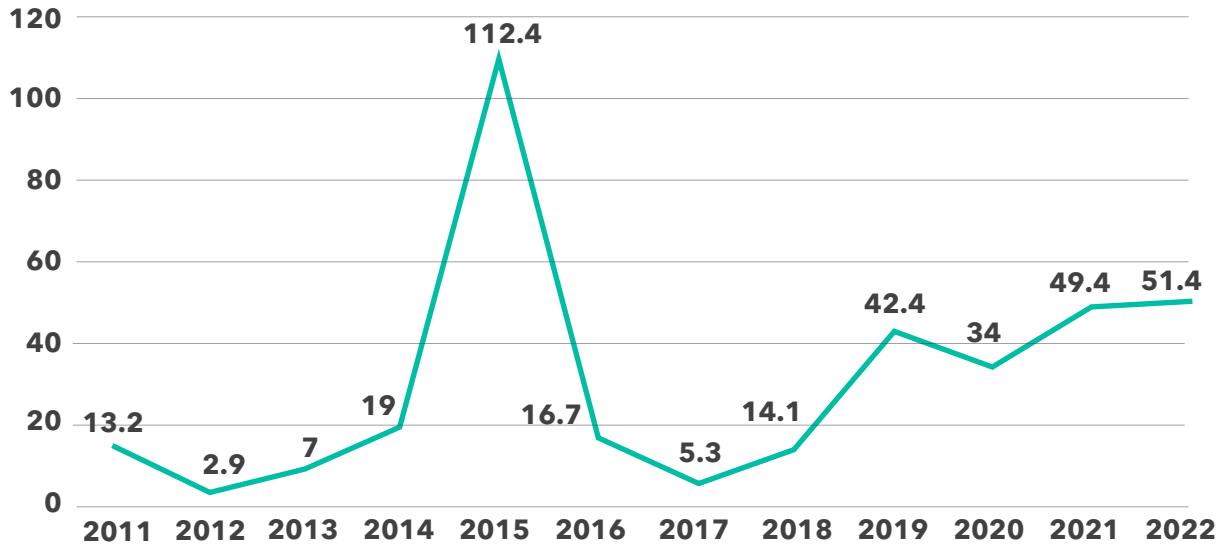
[3] **Source:** https://academynet.com/sites/default/files/q2_insights_briefing_2022_executive_summary_members.pdf

Contents

2022 year in review

Has healthcare finally reached equilibrium in terms of the number of breaches? After a decade of rising breach numbers – a 250% increase from 2011-2021 – the number of breaches decreased slightly in 2022. However, the number of breached records increased to 51.4 million in 2022, compared with 49.4 million in 2021. This is the highest number of record breaches, apart from the anomalous 2015 when just two breaches from Anthem Inc. and Premera Blue Cross affected nearly 90 million records.

Healthcare records breached (in millions)



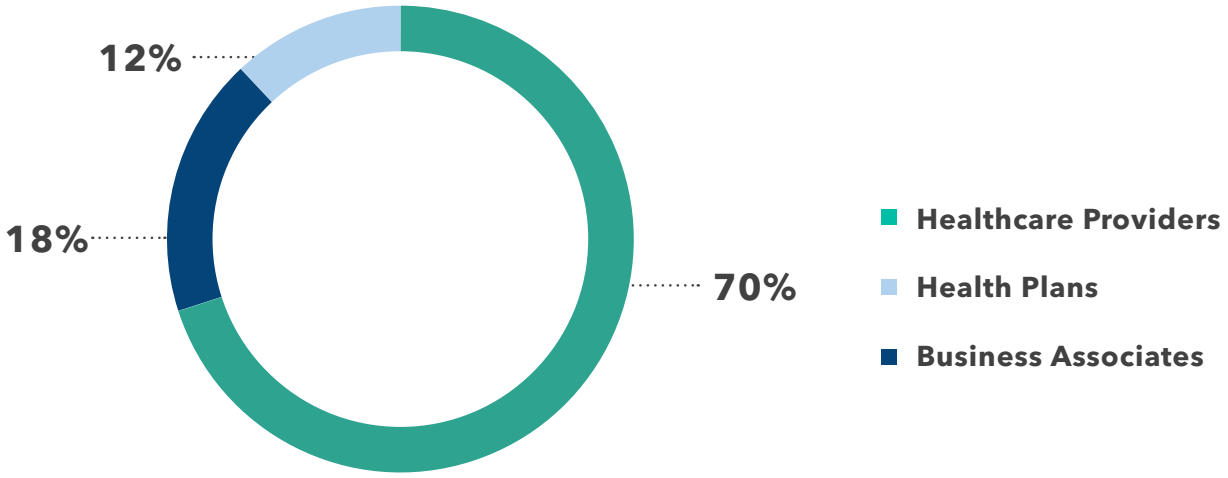
Any breach of 500 or more patient records must be reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).[4] So, while the number of breaches leveled off, the severity of individual breaches is increasingly getting worse, inflicting tremendous damage on healthcare organizations and patients whose records are compromised.

As in past years, healthcare providers represent the majority of breaches, accounting for 70% of all incidents in 2022. Health plan performance improved somewhat, dropping one percentage point to 12%. But the percentage share of breaches attributed to business associates (BAs) increased from 15% in 2021 to 18% in 2022.

Healthcare providers represent the majority of breaches, accounting for 70% of all incidents in 2022.

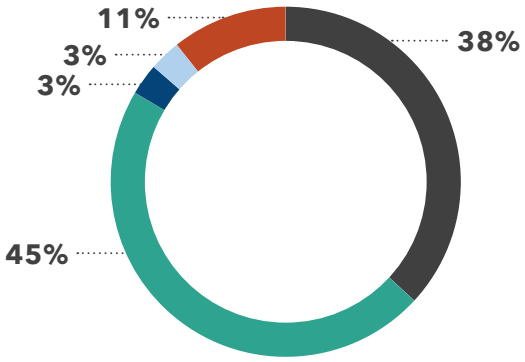
[4] Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Type of entity reporting a breach in 2022

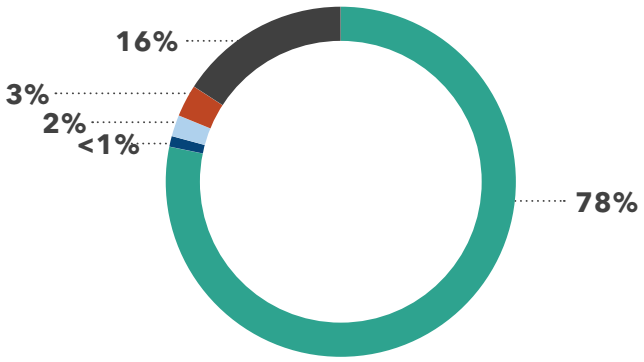


The continued rise in the percentage of breaches attributed to hacking and IT incidents should trouble CISOs and other healthcare security personnel. Until 2018, hacking incidents accounted for fewer than 50% of all breaches. However, the percentage rose from 74% in 2021 to nearly 79% in 2022. The second-largest category is unauthorized access, which dropped from 21% in 2021 to 16% in 2022.

Type of breach in 2018



Type of breach in 2022



Hacking/ IT Incident Unauthorized Access Theft Loss Improper Disposal

Healthcare mirrors cybersecurity trends in other industries, but the potential effects of cybercrimes against healthcare outpace those felt by other industries. The inability, or limited ability, to care for patients because of a security incident pales in comparison to a small charge on a credit card that is easily reversed once identified. But unlike credit card fraud, patient access to healthcare isn't something you can easily walk back.

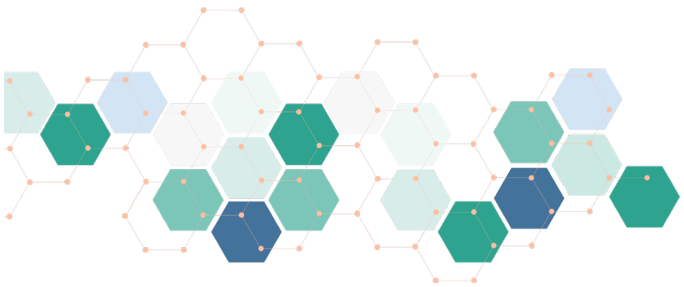
Nearly one-half of respondents to a global survey reported a successful cyberattack in the previous 12 months preventing data access. That figure is a 23% increase from 2021. More than two-thirds lack confidence their protection measures are sufficient to deal with malware or ransomware attacks, and 63% are not very confident their mission-critical data could be reliably recovered after an attack.[5]

Healthcare organizations must get granular with cybersecurity precautions if they want to stem the tide of breaches. Focusing on the basics – strong passwords, multi-factor authentication (MFA), vulnerability management, frequent patching, and managing human risk through continuous training of the entire workforce – will go a long way toward minimizing threats from the inside and outside.

Nearly one-half of respondents to a Dell Global Data Protection Index (GDPI) survey reported a successful cyberattack in the previous 12 months preventing data access – a 23% increase from 2021.

Security check

- Are you aware of, and do you have visibility into your security weak spots across the organization?
- Have you established a corrective action plan to effectively mitigate or remediate your identified risks?
- Do you have a proactive strategic plan – one to three years out – for improving your cybersecurity posture?



[5] Source: https://www.darkreading.com/endpoint/zero-trust-initiatives-stall-cyberattack-costs-1m-per-incident

Top priorities for healthcare cybersecurity in 2023

Right now, 2023 feels much like 2022. Last year's bad actors are still working hard to find new ways to steal from you, while healthcare employees are still working long hours, IT budgets are still stretched thin, and retaining good cybersecurity staff is still a challenge.

But there are ways to minimize risks and maximize your budgeted resources and investments, allowing you to keep providing the level of customer care on which your organization is built. These five priorities can help you do that and help keep your organization's data safe.

1. **Tackling emerging threats**
Today's bad actors increasingly show a remarkable lack of empathy when it comes to their healthcare victims – the impacts of their crimes on patient care take a backseat to illegal profit. Having proactive resources and tools that employ the collective knowledge of the healthcare and cybersecurity industries is critical to preventing threats on the front lines.

2. **Third-party risk management**
Third-party risk management (TPRM) shouldn't be a point-in-time response to a cyber insurance request or a mandate from the C-suite. It should be a comprehensive and forward-looking program, integrated into the overall vendor evaluation process as a proactive engagement of identifying risk versus a reactive approach that happens after vendors are onboarded.

3. **Multi-factor authentication bypass**
Ransomware attacks dipped in Q1 2022 – a decrease partially attributed to a rise in multi-factor authentication. But hackers adapted by targeting smaller businesses less likely to attract attract attention. They're using new methods designed to avoid or exploit MFA and using brute force methods to wear down users. Hospitals and health systems need to continue their vigilance.

4. **Take advantage of available subsidies and grants**
The majority of hospitals operated in the red in 2022, putting pressure on expenses across the organization. Regardless of your hospital size or location, additional federal and state incentives, including subsidies and grants for information technology and cybersecurity programs, may be available to improve your healthcare operations and overall security posture. Some programs exist today, but more help is on the way.

5. **Security awareness training**
Hospitals and health systems need to create a culture of security, given that more than 80% of breaches involve a human element. Once-per-year security training may tick the compliance box, but it is insufficient to create the vigilant internal culture necessary to keep healthcare data safe.

Three tips to combat existing and emerging threats

In December, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released a joint advisory warning industries, including healthcare, that threat actors using Cuba ransomware had infiltrated hundreds of companies.[6]

While the threat was observed as early as November 2019, the pace of attacks picked up in December 2021, with double the number of previous attacks between December and August 2022. Globally, the ransomware attack victimized 100 companies and generated more than $60 million in ransom for criminals.

Just as healthcare is dynamic, so are the cyber threats facing organizations. New threat vectors pop up regulary, requiring vigilance to monitor IT infrastructure, evaluate anomalies, and remediate any discovered weaknesses. Each staff member, device, technology connection, API, and third-party vendor or business associate increases your organizational risk. Unfortunately, attacks are increasing in severity, with hackers demanding multiple ransomware payments, failing to provide access details, publishing data for extortion, or trashing data just because they can.

In September, the FBI outlined three attacks against healthcare organizations that netted more than $4.6 million in ill-gotten gains. The agency said hackers used multiple methods — including publicly available personal details, social engineering, phishing, and spoofing support centers — to impersonate victims and gain access to banking details. In two instances, hackers used credentials from a healthcare company to shift the direct deposit details of a hospital to an account they controlled, stealing $3.8 million. In another, an impersonator was able to change Automated Clearing House (ACH) instructions to swindle another company out of $840,000.[7]

These are but a few examples of the internal and external threats hospitals and health system IT teams deal with daily. IT departments are often cost-constrained, forced to do the bare minimum, or forced to choose among equally important cybersecurity initiatives. Let's face it: cybersecurity is often considered a cost center because it doesn't directly benefit patients. However, breaches often prevent hospitals from delivering care — diverting patients to other facilities, or delaying care for others.

> The pace of attacks picked up in December 2021, with double the number of previous attacks between December and August 2022.

But safeguards exist that can thwart bad actors from exploiting the three key vulnerabilities needed to conduct a successful breach: visibility into a target system, the ability to interact with the target, and the capability to execute on that interaction. Understanding the potential threats and taking proactive steps can help secure your networks.

6 Source: https://healthitsecurity.com/news/cisa-fbi-alert-healthcare-sector-of-cuba-ransomware-tactics
7 Source: https://www.bleepingcomputer.com/news/security/fbi-hackers-steal-millions-from-healthcare-payment-processors/

Know your (IP) range

Your IT systems are under constant scrutiny, whether by search engines benignly trolling so they can create better search functionality or by your internet service provider to see which ports are open so they can manage their own security or prevent improper outbound traffic. These scans return basic information about what operating systems are in use, website coding, and more. But not-so-legitimate people may also be scanning your network, probing for vulnerabilities.

The key to controlling visibility is understanding your IP space, your perimeter, your systems, and your potential weak spots. We've had clients request penetration testing who didn't know their IP ranges, which is critical information they should be able to access easily. Automate your visibility practices to make threat management easier.

Manage password strength

The simplest path into your systems is through a compromised password. Even in organizations using single sign-on (SSO), passwords are often poorly implemented and managed, allowing users to select common words and phrases that hackers can easily break.

In addition to requiring longer passwords and the use of numbers and characters, consider banning the name of local sports teams or other commonalities shared in a locale. And, if possible, restrict the use of the same passwords across devices or logins. Multi-factor authentication, when deployed fully and properly, can provide additional protection from unauthorized logins.

Implement endpoint detection and response

Finally, organizations need to thwart a hacker's ability to execute malicious software or actions within their network. Many organizations still deploy traditional antivirus software, which does a fine job removing known viruses, but does nothing to combat what's known as "living off the land."

> Single sign-on is often poorly implemented. MFA, when properly managed, can provide additional protection from unauthorized logins.

This is a practice where criminals gain access to systems and, rather than causing a big, noticeable scene by immediately launching malware or locking up data, they remain in stealth mode, moving through your network and stealing as much information as they can for as long as they can. And then in true bad-actor fashion, just before they're caught or when they think they have all they can get, they cause a big scene by launching malware or ransomware.

To be truly effective in thwarting attacks, healthcare organizations need to advance their understanding of what response capabilities can bring enhanced detection, not only from a heuristic perspective but also from a behavioral perspective. The result is higher visibility, not simply to quarantine compromised files but also to sever connections with machines that have been accessed in an unauthorized manner. That's why endpoint detection and response (EDR) software is growing in popularity.

Hospitals and health systems make investments every day to improve their facilities, upgrade equipment, and invest in new technologies to enhance patient diagnosis and treatment. Similarly, investing in IT infrastructure is critical to protecting hospital networks, systems, and software, and for maintaining care delivery.

Security Check

- Does your IT staff understand the weaknesses in your network infrastructure?
- What investments are you making to strengthen your defenses?
- How is your organization monitoring and remediating emerging threats?

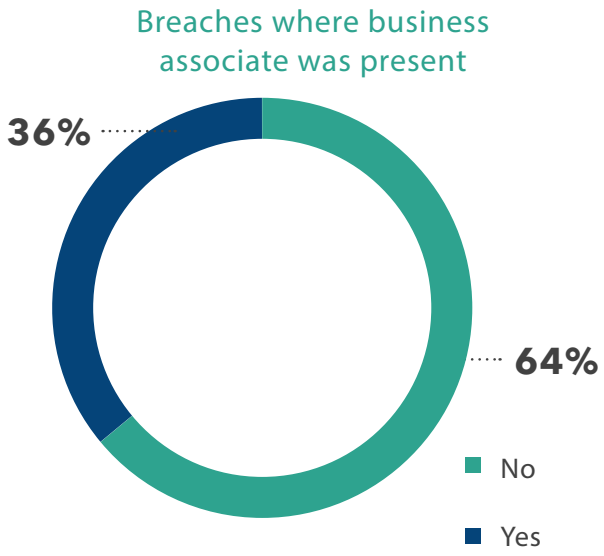
Third-party risk management bolsters protection

In a recent survey, more than half of healthcare organizations reported a third-party data breach in 2022.[8] Worse, 70% of those third-party breaches were caused by granting third parties too much remote access.

While third-party access to organizational data and network resources is critical for hospitals to function properly in an increasingly vendor-supported environment, many organizations fail to secure those connections. Often healthcare risk management programs fail to address security surrounding their third parties due to a lack of automation, partial or non-deployment of security controls, and the time and resources required for conducting risk assessments.

According to breach data from the Office for Civil Rights, a business associate (BA) is present in 36% of healthcare breaches, a percentage that has held steady over the past few years. In addition, BAs are directly responsible for 18% of all breaches, a percentage that is increasing and many of those third-party services involve cloud-hosted solutions.[9]

A significant example of a third-party breach affecting healthcare operations occurred in December 2021, when HR and payroll company Kronos reported a data breach affecting more than eight million customer employees. The breach impacted multiple companies across numerous industries, such as FedEx, Whole Foods, the city of Cleveland, and PepsiCo. The outage included a cloud-based product specifically designed for the 24/7/365 nature of healthcare and used in settings from small rural hospitals to academic medical centers and large healthcare systems.[10]



While healthcare was slower than many industries in moving IT services to the cloud, the modern hospital cannot function without cloud-based services for everything from EHR and PACS to bed management software, medical devices, procurement software, heating and air systems, and much more. Each of those connections presents a potential entry point for bad actors to infiltrate the hospital infrastructure ecosystem and look for ways to move to other systems where sensitive data is stored.

8 Source: https://www.securelink.com/blog/the-state-of-third-party-remote-access-risk/
9 Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
10 Source: https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits

Best practices necessitate a comprehensive TPRM program that's integrated across the organization and throughout the lifecycle of business relationships. This lifecycle begins during vendor selection, continues through onboarding, and only ends when the business associate finishes its relationship with your organization – which should only happen upon and only after completing a checklist of security precautions designed to remove all access to your systems.

Continuous monitoring and re-assessment are critical for effective TPRM to identify security breaches and respond to changes in vendors' security postures. Holding vendors accountable for remediating their security gaps is key to minimizing the likelihood of external risks impacting the organization.

5 steps for managing BA risk

- Prioritize the evaluation of existing BAs by risk potential
- Thoroughly vet new BAs before entering into agreements
- Continuous monitoring and risk assessment
- Enforce a BA cybersecurity exit strategy

Identifying which vendors to assess initially as part of the TPRM program should consider a broad range of risk factors. Systems that facilitate patient care, require an elevated level of availability, store, process, or transmit sensitive data, or support critical business processes should be included within third-party risk management. Think EHR, lab systems, pharmacy, imaging, OR/ER systems, and communications. But sooner, rather than later, every third-party system connected to your network or handling sensitive data must be evaluated. The evaluation process includes contacting each vendor and documenting their security practices as they relate to your organization. If they are not sufficiently secure, what steps are required to bring them into compliance?

Chasing down vendors, reviewing documentation, verifying attestations, documenting risks and corrective action plans, conducting follow-up evaluations, and monitoring ongoing connections can stress even the largest health systems. That's why organizations use managed security services providers to perform TPRM services. Fortified's TPRM assessment methodology is based on industry-accepted frameworks and relevant regulatory requirements that ensure vendor assessments are executed and evaluated consistently.

Security check

- How does your organization track its third-party assets?
- What measures are you taking to ensure connections with third parties are secure?
- Can you adequately manage your TPRM program internally?

Hackers pivot to bypass MFA protocols

A dip in ransomware incidents in Q1 2022 was initially hailed as a triumph of multi-factor authentication (MFA) over criminals. However, other changes in the industry are possible contributors to the dip. For instance, insurance companies increasingly require MFA as a precursor to offering cyber insurance, leading to more companies adopting the technology.[11] Likewise, media coverage and federal efforts to bolster cybersecurity are credited with playing roles in the perceived decrease.

Ransomware is a $6 trillion business, so it's not going away anytime soon. Another report shows ransomware increasing by 41% year over year, leaving little doubt that it will remain a viable attack vector in the future.[12] The threat landscape is ever-changing, and criminals are getting organized.

The existence of Initial Access Brokers (IAB) sheds new light on evolving tactics for circumventing security controls. Arguably, an IAB's biggest barrier to criminal entry is MFA, meaning most of their attention will focus on trying to bypass it completely. To do this, criminals target exploitable vulnerabilities and policy configurations, using highly effective social engineering tactics and employing brute force methods to wear down users.

It's commonplace in today's security culture to simply accept that there will always be a gap between our best-case security posture and our current environment. While this idea is pervasive, it is detrimental to the security of our authentication processes. Like any other tool in your technology stack, MFA requires proper care and feeding to ensure it's delivering maximum value for an organization.

During many penetration tests and threat-hunting exercises, Fortified analysts often find vulnerabilities or configuration issues proving MFA was not maintained or implemented properly. Remediating these problems can be as simple as discovering and patching unpatched systems to remove exploitable vulnerabilities, and as complex as implementing periodic policy reviews to ensure that only proper authentication pathways are open.

> Ransomware is a $6 trillion business, with reports of it increasing by 41% year over year.

Human nature dictates that users will always be a security risk. We hire people based on their ability to complete job functions, and often that doesn't include cyber literacy. Our adversaries understand this and prey on these shortcomings using well-known but highly effective social engineering tactics. Impersonating a C-level executive who "just received a new phone" and needs to reset their MFA relies on the same urgency and fear responses as common phishing techniques.

11 Source: https://www.channelfutures.com/from-the-industry/the-ransomware-threat-is-it-decreasing-or-retargeting
12 Source: https://www.securitymagazine.com/articles/98668-how-businesses-can-prevent-becoming-the-next-ransomware-victim

Humans are susceptible to brute-force attacks. MFA bombing involves sending multiple authentication requests, often push notifications, to the same user. The rationale is that the person will eventually give in, hoping that acceptance will stop the nagging. These social engineering and brute-force tactics are increasingly effective among healthcare employees, as they battle burnout from post-COVID staffing shortages and particularly busy flu seasons.

With all the ways attackers try to circumvent MFA technologies, what are some reasonable ways to prepare and prevent this activity? The best defense for hospitals and health systems is to focus on the basics of cybersecurity.

The basics of cybersecurity include:

- Keeping patches updated
- Periodic technology policy reviews
- Periodic risk assessments to understand security gaps
- Regular penetration tests to understand exploit paths in your environment
- A mature security operations center (SOC) with reactive playbooks and proactive threat hunting
- Up-to-date endpoint protection controls to allow for defense in depth

Security check

- Has your organization deployed MFA everywhere possible?
- What steps are you taking to prevent MFA bypass?
- How are you educating employees about potential cybersecurity risks?

Does your hospital qualify for subsidies or grants?

Large and small hospitals and health systems throughout the country face intense budgetary pressures. According to a fall 2022 report prepared by Kaufman Hall for the American Hospital Association, more than half of hospitals report negative margins relative to pre-pandemic levels. At the same time, expenses have increased significantly, with labor increasing $86 billion over 2021 and non-labor expenses $49 billion higher.[13]

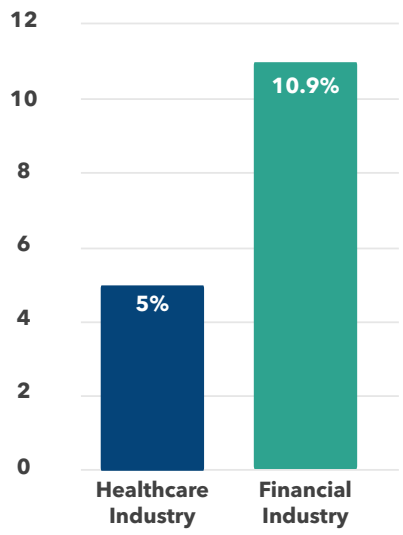
While it's obvious that patient care should be a higher priority than cybersecurity, that doesn't mean C-suites shouldn't prioritize cybersecurity spending. Healthcare continues to underspend on cybersecurity compared to other industries – despite incurring the highest costs to remediate data breaches for 12 years running. Since 2020, remediation costs have increased by 42% to just over $10 million per incident.[14]

According to estimates, healthcare organizations spend about 5% of their IT budgets on cybersecurity. In comparison, the financial services industry (the second worst industry in terms of breach remediation costs), dedicates 10.9% of IT budgets to cybersecurity spending.[15] A 2021 HIMSS survey showed that 73% of respondents thought their healthcare organization should increase cybersecurity spending while just 40% believed their organization had the funding to make those investments.[16]

Compounding those problems, rural hospitals have been particularly hard hit by the pandemic and its financial aftermath. The resource constraints all hospitals face are exacerbated in rural settings. Employees in all departments, not just IT, are harder to find and keep, and rural hospitals' financial challenges forced the closure of 136 facilities in the last 11 years, including 19 in 2020 alone.[17]

The healthcare industry has been abuzz since Virginia Sen. Mark Warner released the *Cybersecurity is Patient Safety* policy paper in November, which outlines the security threats facing the healthcare industry and includes proposals to assist facilities in all aspects of cyber spending, from startup funds to disaster recovery assistance following a breach or attack.[18]

Cybersecurity spend within total IT budgets



13 Source: https://www.kaufmanhall.com/insights/research-report/current-state-hospital-finances-fall-2022-update
14 Source: https://www.ibm.com/reports/data-breach
15 Source: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html
16 Source: https://www.himss.org/news/himss-research-how-cybersecurity-priorities-have-shifted-response-covid-19
17 Source: https://www.aha.org/news/headline/2022-09-08-aha-report-rural-hospital-closures-threaten-patient-access-care
18 Source: https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf

However, a proposal isn't a law or even a mandate. So, while it's exciting that Congress is paying attention to healthcare cybersecurity, the excitement won't scan for vulnerabilities or patch software.

There is already some money available for hospitals and health systems from federal and state grants and subsidies designed to help organizations develop and maintain their cybersecurity programs. At Fortified, we are working hard to raise awareness among our partners that these programs exist. While not all hospitals will be eligible for every funding option, it's vitally important to take advantage of existing funding if your organization qualifies and to watch for new funding opportunities in the pipeline.

Existing resources and funding options:

Federal Communications Commission

Healthcare Connect Fund. Administered by the Federal Communications Commission, the Healthcare Connect Fund administers $150 million in annual funding to expand access to broadband services, especially in rural areas, and to encourage the formation of state and regional broadband networks linking healthcare providers. Not a rural hospital? If you join a consortium that's at least 50% rural, you may qualify. The fund pays for 65% of a project, with the facility responsible for the remainder. Since heightened connections would include network management, network oversight, and software to help monitor or protect the connections, some cybersecurity funding could be covered.[19]

FEMA

Homeland Security Grant Program. There are a variety of grants available through each state's Homeland Security Grant Program for which facilities may qualify. The State Homeland Security Program (SHSP) targets state and local government organizations, which many state and county hospitals would qualify for. There are also several grants available to nonprofit organizations under the Nonprofit Security Grant Program (NSGP). The Federal Emergency Management Agency (FEMA) provides information on how to contact your state office.[20]

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

State and Local Cybersecurity Grant Program. This federal program applies to local, state, regional, and tribal hospitals, among other government facilities, that need help addressing cybersecurity risks and data protection. The fund is administered by the Cybersecurity & Infrastructure Security Agency. In 2021, Congress authorized $1 billion in awards over a four-year period to eligible facilities.[21]

19 Source: https://www.fcc.gov/general/healthcare-connect-fund-frequently-asked-questions#Q38
20 Source: https://www.fema.gov/grants/preparedness/nonprofit-security
21 Source: https://www.cisa.gov/cybergrants

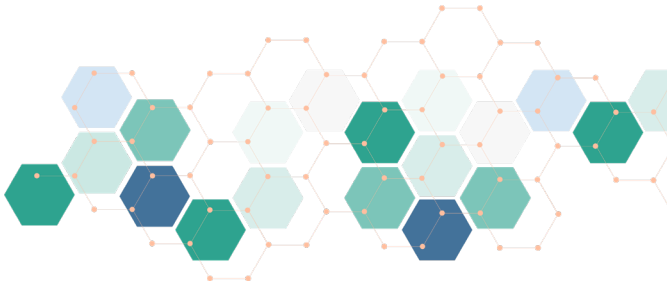
Health IT Privacy and Security Resources for Providers, the Health Sector Coordinating Council,[22] the Cybersecurity Infrastructure & Security Association (CISA),[23] the Health Information Sharing and Analysis Center (H-ISAC),[24] 405(d),[25] the Administration for Strategic Response (ASPR),[26] and CHIME[27] are among organizations that have banded together to develop tools, guidance documents, and educational materials to assist healthcare providers in adopting a robust security posture.

Other state and local grants. Many states and municipalities have subsidies and/or grants that hospitals may be eligible for. It may take a little digging to find what you're looking for, but it would be well worth the effort if you're successful. Ask CIOs or IT executives at other institutions about potential funding sources.

At Fortified Health Security, we recently increased our efforts to raise awareness about subsidies and grants that can help defray some of the costs of hospital cybersecurity programs. If you need assistance identifying funding possibilities, please contact us.

Security check

- What percentage of your IT budget is spent on cybersecurity?
- What cybersecurity projects do you consider critical for your organization?
- Have you explored subsidies or grants to help defray IT infrastructure and cybersecurity costs?



22 Source: https://healthsectorcouncil.org/hscc-publications/
23 Source: https://www.cisa.gov/
24 Source: https://h-isac.org/
25 Source: https://405d.hhs.gov/resources
26 Source: https://aspr.hhs.gov/Tools/Pages/default.aspx
27 Source: https://chimecentral.org/public-policy/cybersecurity-resources/

Create a culture of security in your organization

It's a fact: More than 80% of data breaches involve a human in some way. That could involve someone falling for a spear-phishing campaign designed to solicit credentials, clicking on a malicious link, or a simple error that leaves a security vulnerability open to bad actors.[28] Creating a culture of security in your organization will keep security at the forefront of everything from operations to care delivery.

Monitoring and maintaining the security of IT infrastructure is often overemphasized within hospitals and health systems, while the human side of reducing risk is often under-emphasized. And unlike APIs, software, and technology hardware, employees can't be patched; they can't be reconfigured; and they can't be reset after making a mistake.

The answer is training, continual training to help create a culture of security within your hospital or health system. But with so many competing training programs – everything from HIPAA and regulatory compliance to handwashing and job-specific training – it's difficult to break through the noise and gain traction. But as the average recovery cost for a healthcare organization after a breach has now passed the $10 million mark in 2022, a 40% increase from 2020, the time for definitive action is now.[29]

If a doctor, nurse, or other hospital employee sees a suspicious package in a hallway, chances are good they will alert the physical security department who will take appropriate measures. But what about a suspicious email? Some IT departments don't want to know, believing it's just more work for them. But for every potentially damaging email that's deleted without taking any action, there could be thousands more in waiting.

> Because the average recovery cost for a healthcare organization after a breach has now passed the $10 million mark, a 40% increase from 2020, the time for action is now.

The key to creating a mature and robust security awareness program starts with executive leadership support, followed by continual training to reinforce the security message. Across industries, some companies have a dedicated position for security awareness or give an existing IT person some additional duties as a security awareness officer. With continued IT staffing shortages in healthcare, that might not be possible, so consider outsourcing security awareness and training to a vendor well-versed in the unique nature of healthcare.

Some healthcare organizations are minimally training their staff for compliance, hoping it will be sufficient. But minimal training delivered once a year can't address the dynamic nature of cyber threats, which are continually evolving. As organizations harden their security posture in response to specific threats, new threats emerge that companies may not be aware of.

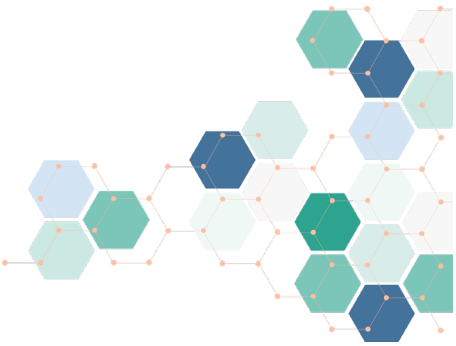
[28] Source: https://www.verizon.com/business/resources/reports/dbir/
[29] Source: https://www.ibm.com/reports/data-breach

Two recent emerging threats:

- In August, the FBI warned healthcare organizations about a fraud scheme where scammers impersonate law enforcement or government personnel, targeting specific individuals to extort money or steal personally identifiable information. The scammers spoof authentic phone numbers and use names of real security personnel, informing the target they missed a court date and owe a fine or are subject to arrest unless they comply.[30]

- The following month, a new, sophisticated phishing attack was revealed, using multiple fake email accounts to trick a user into believing he/she is part of a conversation among colleagues. Called multi-persona impersonation, multiple interactions take place to convince the target the conversation is real before a malicious link is sent. The "grooming" process can take weeks, underscoring the lengths hackers will go to steal information.[31]

The SANS Institute, a leading authority on cybersecurity training, certifications, and resources, recommends monthly training noting, "Organizations that engage and train their workforce only annually or on an ad hoc basis cannot effectively change behavior and are thus stuck at the compliance level, checking the box." The information security organization recommends monthly training that's "communicated engagingly and positively that encourages behavioral change" to help employees understand the importance of cybersecurity so that they will actively recognize, prevent, and report incidents.[32]



Training doesn't have to be overly formal. Some of the most effective training involves humorous videos depicting fictional hospital employees failing at HIPAA security or allowing someone to openly walk through administrative areas simply because they have an official-looking badge. This kind of training connects with trainees, offering better retention and creating an "a-ha!" moment when they are later faced with a similar situation.

To make it more fun, you might hold a prize drawing among those who report a potential security incident during a certain time period. The key is a constant drumbeat of training that helps create the culture of security that healthcare organizations need.

30 Source: https://www.fbi.gov/contact-us/field-offices/baltimore/news/press-releases/fbi-warns-individuals-employed-in-the-healthcare-industry-of-the-ongoing-scam-involving-the-impersonation-of-law-enforcement-and-government-officials
31 Source: https://www.pcgamer.com/hackers-are-improving-phishing-attacks-by-having-you-chat-with-sock-puppets/
32 Source: https://www.sans.org/

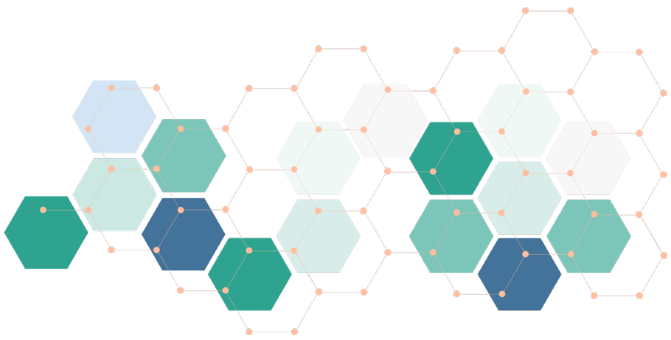
To build on the training, phishing exercises carried out by your organization's security group can help gauge the effectiveness of the training. Users who struggle with identifying phishing scams should receive additional training. Phishing training is complex and requires purpose-built tools, such as education software designed to be impactful, but also something employees don't dread. Phishing education software can also give IT tools to create fake emails, and some vendors provide dashboards or other metrics to determine effectiveness by employee or department. Third-party vendors can also conduct phishing campaigns on behalf of organizations.

Fortified's recommendation is to phish each employee at least once a quarter. Some healthcare organizations phish everyone during a limited time, which can create bottlenecks for IT staff. Consider a drip email campaign of weekly or bi-weekly emails that phish each employee quarterly.

Creating a culture of security is critical for hospitals and health systems, as important as the physical security of network infrastructure, monitoring network traffic, and maintaining a robust software patching program. Given the tight IT workforce environment and competing demands on existing IT staff, outsourcing a managed security awareness and training program might make sense.

Security check

- How are you managing the human risk angle of cybersecurity?
- Is your current security awareness program effective? How do you measure success?
- How often do employees receive cybersecurity training?



Cybersecurity outlook for 2023

What do we expect to see in 2023? Here are some key areas to watch:

Increased cybersecurity funds for providers

We believe healthcare cybersecurity is at a tipping point. More than 49 million breached patient records each of the past two years is generating a great deal of attention at the federal level. We expect additional funding support for continuing efforts to help healthcare organizations secure their technology infrastructure.

Cybersecurity spending will increase

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. A survey of leading health systems showed greater interest in increasing cyber spending (93%), than clinical staff (81%), cloud migration (81%), or ambulatory capital projects (90%).[33]

Expect more large-scale breaches

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. The sheer number of connections among healthcare IT infrastructure and the value of protected health information on the black market continues to make the industry an attractive target.

Continued IT talent crunch brings more MSSP partnerships

IT talent challenges across industries have hit healthcare particularly hard. That's not expected to ease in 2023. The labor shortage will accentuate the value of managed security services providers to handle both day-to-day cybersecurity tasks and more sophisticated deployments while supplementing existing IT staff.

[33] Source: https://academynet.com/sites/default/files/q2_insights_briefing_2022_executive_summary_members.pdf

Moving forward

How can you keep moving your cybersecurity program forward? Here are some tips.

Focus on the basics

Like nearly every aspect of our lives, the threats and challenges to healthcare IT environments seemingly grow in severity and potential impact daily. However, don't overlook the basic blocking and tackling that can prevent most breaches: user access management, appropriate network log review, and prompt patching of software vulnerabilities. Taking care of those three tasks goes a long way toward protecting your organization's IT infrastructure.

Continuous staff training

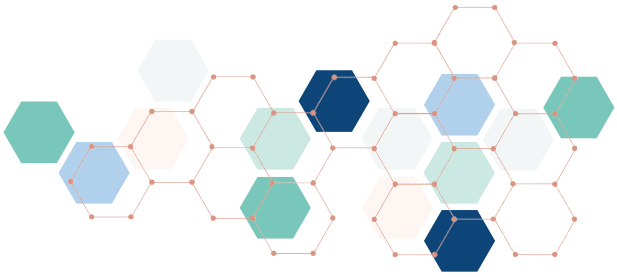
All of us in IT know that one errant click on a malicious web link by an inattentive employee can bring a hospital to its knees and cripple its ability to care for patients. Most breaches involve a human element, making your staff the weak link. Train new hires. Train all users regularly. Phish to verify. Measure your effectiveness. Retrain those who need it.

Stay positive

We believe that government funding to help hospitals secure their IT networks is on its way. If possible, contact your state and federal lawmakers and tell your cybersecurity story, outline the challenges your organization faces, and tell them what resources you need to adequately protect your networks. Change is coming.

Leverage your peer community

What's working in your organization and what can you do better? Fortified's monthly roundtable events[34] set the stage for peer learning and networking in a comfortable environment. There are no sales pitches or vendor tie-ins, just an opportunity to share security tips, tricks, and best practices for the betterment of your organization.



[34] Source: https://fortifiedhealthsecurity.com/fortifiedroundtables/

Were we right?

Each year, we like to stop and look at the prior year's predictions and see how they compared with what happened. Here's a look at Fortified's 2022 Predictions:

Prediction 1

Number, severity of breaches grows: The number of healthcare data breaches will continue to rise, along with an increased attack severity that will put hospitals under pressure.

How did we do?

The number of breaches held steady in 2022 while the number of affected records increased, so this prediction proved to be a mixed bag. However, the average number of breached records between 2019-2022 is more than 44 million annually, a nearly three-fold jump from 2018.

Prediction 2

SolarWinds of healthcare: A breach at a third-party vendor that services hospitals and health systems will occur, leaving dozens or hundreds of hospitals vulnerable.

How did we do?

Although the Kronos breach occurred in December 2021, the effects continued to be felt into 2022 by many hospitals and health systems that rely on a third-party vendor for payroll services.[35] This breach underscores the need for organizations to have visibility into every IT system that's connected, however peripherally, to their networks.

Prediction 3

Adoption of EDR solutions grows: More healthcare organizations will recognize the value of endpoint detection and response (EDR) solutions to improve their security strategies.

How did we do?

While it's unclear whether healthcare organizations recognize the value of EDR solutions, cybersecurity insurance companies certainly do, making it a common requirement for securing a cyber policy. Next-generation antivirus solutions are also getting significant traction in healthcare.

Prediction 4

More partnering with MSSPs: Difficulty attracting and retaining security personnel and the recognition that IT security is not a hospital core competency will spur wider alignment between hospitals and MSSPs.

How did we do?

The labor shortages plaguing the cybersecurity workforce have shown no signs of abating, with turnover among IT staff (13.2%) higher than in any other industry (10.5%)[36]. Healthcare IT staff have been traditionally difficult to recruit and retain, owing to the location of some hospitals, long hours, and little upward mobility. Those factors point to the utility that managed security services providers offer to the industry, a trend we expect to continue.

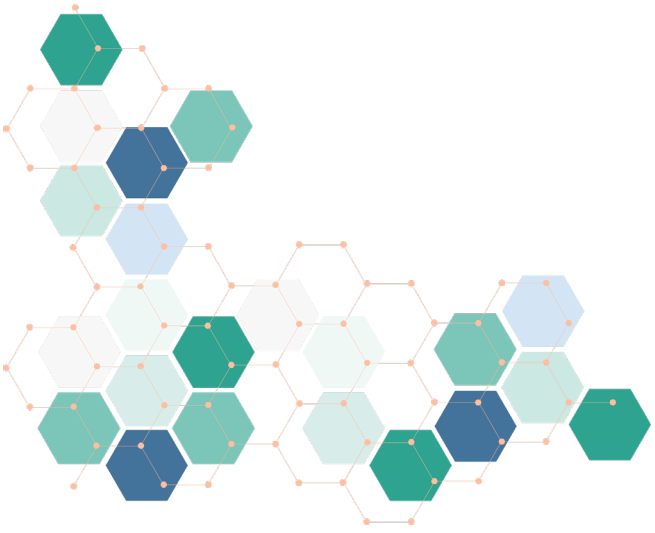
35 Source: https://healthitsecurity.com/news/lasting-effects-of-kronos-cyberattack-ripple-through-healthcare
36 Source: https://www.sterlingcheck.com/blog/2022/01/2022-tech-trends-impact-the-great-resignation/

Conclusion

We hope this 2023 version of the Horizon Report is both impactful and educational. It is informed, in no small part, by the relationships forged between our clients and our sales, security, delivery, and service associates who work closely with our clients every day, and who live and breathe cyber security alongside them.

The outlook for healthcare cybersecurity in 2023 remains cautiously optimistic. Cautious because the threats are real and the bad actors are motivated. But optimistic because cybersecurity awareness in healthcare as a whole, is growing and there are more resources available than ever before to identify and stop threats before they impact the business of providing expert, uninterrupted care to patients.

As always, we encourage you to contact us anytime you have a question, or just want to talk about today's cybersecurity landscape!



About the contributors

Dan L. Dodson
CEO
Fortified Health Security

Dan serves as CEO of Fortified Health Security. For more than 17 years, he's led healthcare and insurance organizations – serving as Executive Vice President for Santa Rosa Consulting, Global Healthcare Strategy Lead for Dell Services, and holding leadership positions with 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 mitigation are regularly featured in popular media and trade publications such *Becker's Hospital Review*, *Healthcare Business Today*, and *Healthcare Innovation News*.

William Crank
COO
Fortified Health Security

William serves as COO of Fortified Health Security. For nearly 20 years, he's driven the successful execution of cybersecurity strategies and tactics for the healthcare industry, including managing the Information Security Risk Management (ISRM) team at Hospital Corporation of America (HCA) and serving as Chief Information Security Officer (CISO) at MEDHOST.

He currently holds multiple 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.

Tim (T.J.) Ramsey
Director, Threat Assessment Operations
Fortified Health Security

With more than 16 years in military intelligence and IT security, T.J. has extensive knowledge of IT security principles, including network hardening and compliance requirements, and is skilled at implementing security solutions for network enterprises.

Daniel Hudgins
Service Lead, TPRM
Fortified Health Security

For more than 14 years, Daniel has worked in healthcare IT for surgery centers and hospitals. He has extensive knowledge and experience in healthcare IT support, EHR implementations, HITRUST, NIST CSF, HIPAA Risk Assessments, and Third-Party Risk Management.

Melissa Adams
Director, TPRM & HITRUST Assessment Services
Fortified Health Security

Melissa has more than 20 years of experience in information security compliance within the healthcare industry including audit and consulting services with major healthcare systems and individual healthcare entities. Her areas of expertise center around leveraging security frameworks for risk assessment and risk management, third-party risk management, HITRUST CSF certification programs, and Information Security Program development and maturity.

Preston Duren
Vice President, Cybersecurity Operations
Fortified Health Security

Preston has more than 15 years of experience in healthcare information security and managed security services, giving him a unique understanding of hospital operations and information security. He has a proven track record of transforming technical operations and building strategic solutions for healthcare organizations.

Jake Bice
Senior Manager, Cybersecurity Operations
Fortified Health Security

For more than six years, Jake has worked in IT and is committed to improving healthcare security. He's adept at administering and implementing firewalls, endpoint controls (Antivirus & EDR), SIEM, and IoMT technologies.

Russell Teague
Vice President, Advisory Services & Threat Operations
Fortified Health Security

Russell is a senior business leader with more than 25 years of experience in U.S. Army Intelligence and Security Command (INSCOM), IT security, cybersecurity, and Information Protection. His background spans various industries, including healthcare, pharma, life science, finance, retail, technology, manufacturing, and oil & gas sectors.

Kate Pierce
Senior Virtual Information Security Officer
Fortified Health Security

Kate has more than 21 years of experience in healthcare IT, with a focus on HIPAA and cybersecurity. Her broad experience in healthcare security as a former CIO & CISO includes a variety of areas, such as security strategic planning, governance, policy and procedure development, executive-level reporting, change management, and staff education and training.

Don Kelly
Manager, VISP & VISO
Fortified Health Security

With more than 15 years in healthcare information security and communications, Don has extensive healthcare-specific experience developing and directing cybersecurity awareness and training programs, performing security strategic planning, incident response program development, risk analysis, and business impact assessments. He currently holds the GISP, GSTRT, GCCC, and the CISSP certifications.

Learn more. Contact us at:

fortifiedhealthsecurity.com

1 (615) 600-4002

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.

For more information visit **www.fortifiedhealthsecurity.com**.

Fortified HEALTH SECURITY

Healthcare's Cybersecurity Partner®

BEST IN KLAS SECURITY & PRIVACY MANAGED SERVICES 2022

MEDTECH BREAKTHROUGH AWARD 2022 BEST OVERALL HEALTHCARE CYBERSECURITY COMPANY

TOP WORK PLACES 2022 Tennessean.

Modern Healthcare Best Places to Work™ 2021 – 2022

fortifiedhealthsecurity.com

2550 Meridian Blvd, Suite 190
Franklin, TN 37067