Fortified HEALTH SECURITY

2023 MID-YEAR

# HORIZON REPORT

The State of Cybersecurity in Healthcare

# CEO's Message

The first half of 2023 has presented hospitals and health systems with a host of challenges that are hard to ignore. From staffing and budget constraints to technological and cybersecurity limitations, the task of ensuring patient safety and data protection has become increasingly demanding.

Fortunately, these obstacles have not gone unnoticed or unaddressed. The federal government is actively taking initiative on the legislative front to tackle these issues head-on.

Kate Pierce, Senior Virtual Information Security Officer at Fortified, was invited to speak before the U.S. Senate's Homeland Security and Government Affairs Committee in March, shedding light on the cybersecurity risks faced by healthcare facilities, particularly smaller and rural ones. Kate has also contributed an article in this report, where she discusses the current landscape and offers proactive measures you can take to prepare for potential threats.

As the federal government works towards greater interoperability to enhance patient care coordination, it inadvertently puts additional strain on cyber security programs. Recent survey findings reveal that independent and critical access hospitals, with limited resources at their disposal, are significantly less likely (by 50%) to engage in health information exchanges. Meanwhile, the Office of National Coordinator has proposed nearly 600 pages of new rules aimed at advancing care initiatives through technology and interoperability.

In this 2023 Mid-Year Horizon Report, we delve into the significant cybersecurity issues that are affecting the healthcare industry. We cover topics such as emerging data theft tactics, the use of risk-based identity alerting to strengthen security, and the potential impact of using ChatGPT on healthcare data security.

We hope this mid-year report provides you with valuable insights into the current state of cybersecurity in healthcare and equips you with practical steps to safeguard patient data.

As always, we value your feedback and perspective. Please don't hesitate to reach out to us at **connect@fortifiedhealthsecurity.com**.

Regards,

Dan L. Dodson


# Contents

# 2023 Mid-Year in Review

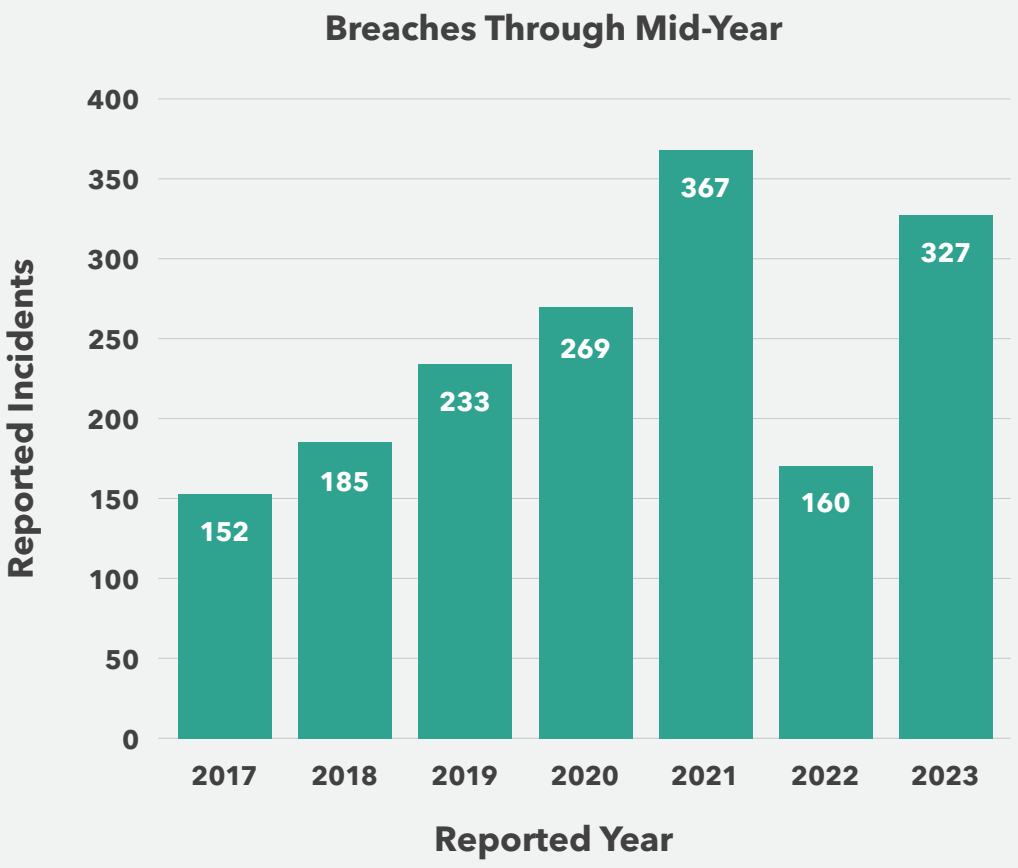
## Breaches

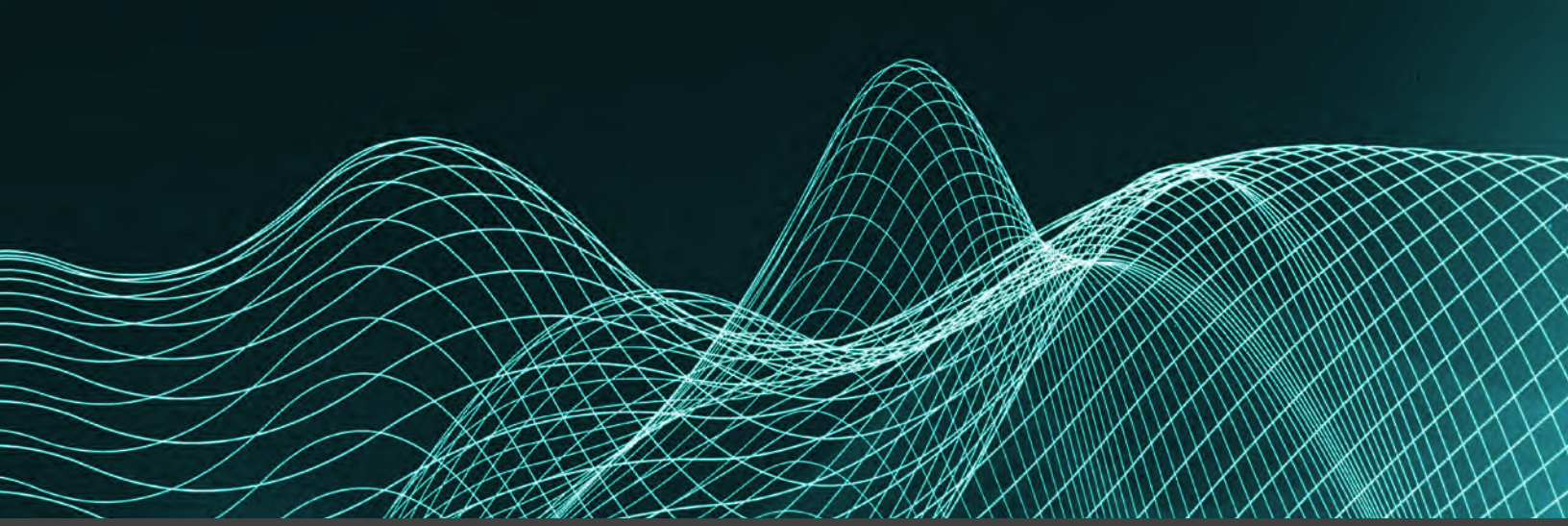
Since the start of 2023, over 300 data breaches have been reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights, an increase of more than 104% compared to mid-year 2022. The staggering rise in breaches has affected over 40M individuals, a year-over-year (YoY) increase of 60%.

**40M+**

**individuals have been affected by breaches since the start of 2023.**

For context, by mid-year 2022, 2 million records had been compromised from a single breach. In the first six months of 2023, five breaches of at least 3 million records each were reported, including a breach of over 8.8 million records at a Georgia-based business associate (BA). Those five incidents comprise nearly two-thirds of the total number of breached records.





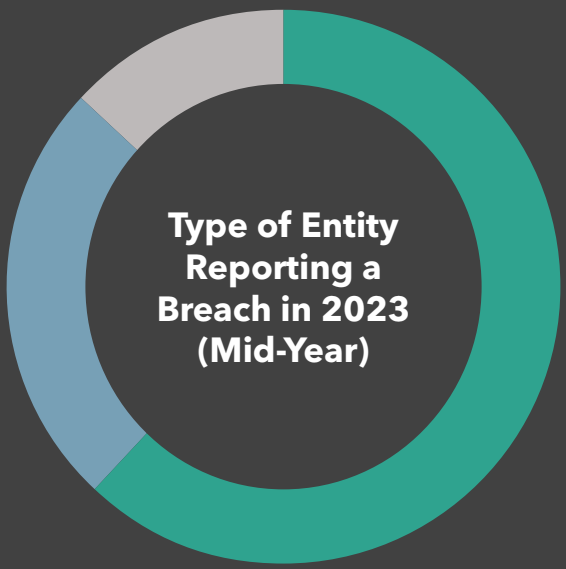
Data security in the healthcare supply chain continues to make headlines, primarily driven by the recent breach of **Fortra's GoAnywhere** secure file transfer software in February. This incident resulted in over 5 million healthcare records being compromised and reported to OCR (Office for Civil Rights). Victims affected by this attack include a supplemental benefits provider, a virtual behavioral health provider, and a large hospital system. The software is used across industries, and many other non-healthcare-specific companies were among the **more than 130 companies** allegedly targeted in the attack.

Even before the Fortra breach, the healthcare industry had been advocating for the adoption of a software bill of materials (**SBOM**) to bring more transparency to healthcare IT networks by listing the components that comprise a piece of software. Much of the healthcare push is in support of the Food and Drug Administration's (FDA) effort on **medical devices**, but the entire supply chain – and not just in healthcare – could benefit from greater transparency.

**273%**

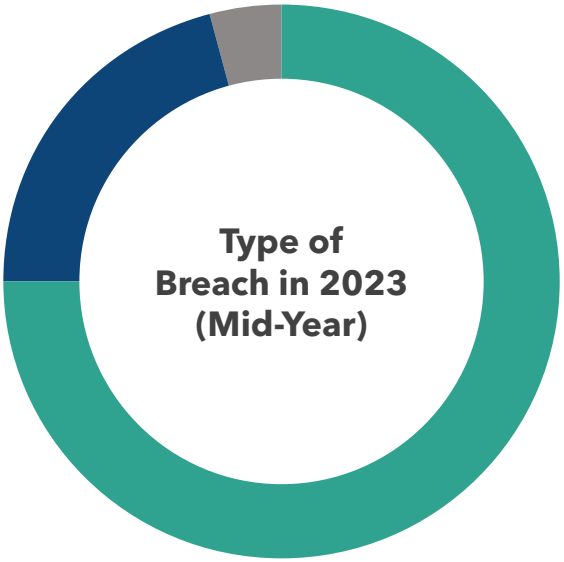
**BA breaches have skyrocketed by 273% YoY.**

Considering the growing prevalence of business associate (BA) breaches, increased focus on the supply chain and third-party risk is critical for hospitals and health systems. At mid-year 2022, BA breaches accounted for 14% of all reported breaches. By mid-year 2023, the number of BA breaches skyrocketed 273%, from 22 to 82. Based on these figures, business associate breaches account for 25% of all hospital and health system breaches. Interestingly, the number of incidents reported by healthcare providers decreased, while health plan breaches remained stable at 13% of the total.

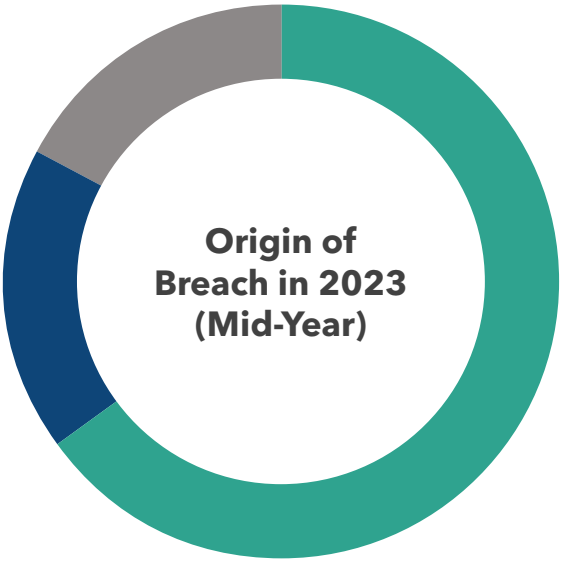



**62%** Healthcare Providers
**25%** Business Associates
**13%** Health Plans

**Of the breaches reported by mid-year 2023, 75% were attributed to hacking, and 21% were from unauthorized access or disclosure (a mid-YoY growth of 133%). As for the origin of these breaches, 65% were from network servers and 18% were from email.**




**75%** Hacking / IT Incident
**21%** Unauthorized Access
**4%** Other




**65%** Network Server
**18%** Email Accounts
**17%** Other

The relentless uptick of cyber threats targeting healthcare organizations and patients shows no signs of abating. This mid-year data underscores the growing challenge posed by third-party risks stemming from business associates (BAs) and implemented technologies.

However, there is a glimmer of hope amidst this grim landscape. Efforts and resources devoted to bolstering healthcare cybersecurity are on the rise. Esteemed healthcare advocacy groups such as HSCC, 405(d), CHIME, H-ISAC, and CISA continue to expand their supply of practical resources. These organizations not only offer educational materials but also extend financial assistance, empowering healthcare entities to counteract the activities of malicious actors.

By working together and leveraging the available resources, educational initiatives, and funding assistance, we can forge a more secure future for the healthcare industry and safeguard the well-being of patients.

# Building Momentum: Legislative Progress and Priorities in Healthcare Cybersecurity

**Over the past six months, healthcare cybersecurity has garnered significant attention from lawmakers in Washington, D.C.**

Perhaps the increased awareness was triggered by the cyberattack on **CommonSpirit Health** – a network of 143 hospitals across 23 states – last fall.

The impact of this attack was substantial, affecting more than 623,000 patients (about half the population of Hawaii), and incurring an estimated recovery cost exceeding **$160 million**. Some experts have even likened it to the **"Colonial Pipeline" ransomware incident** that captured headlines around the world in 2021.

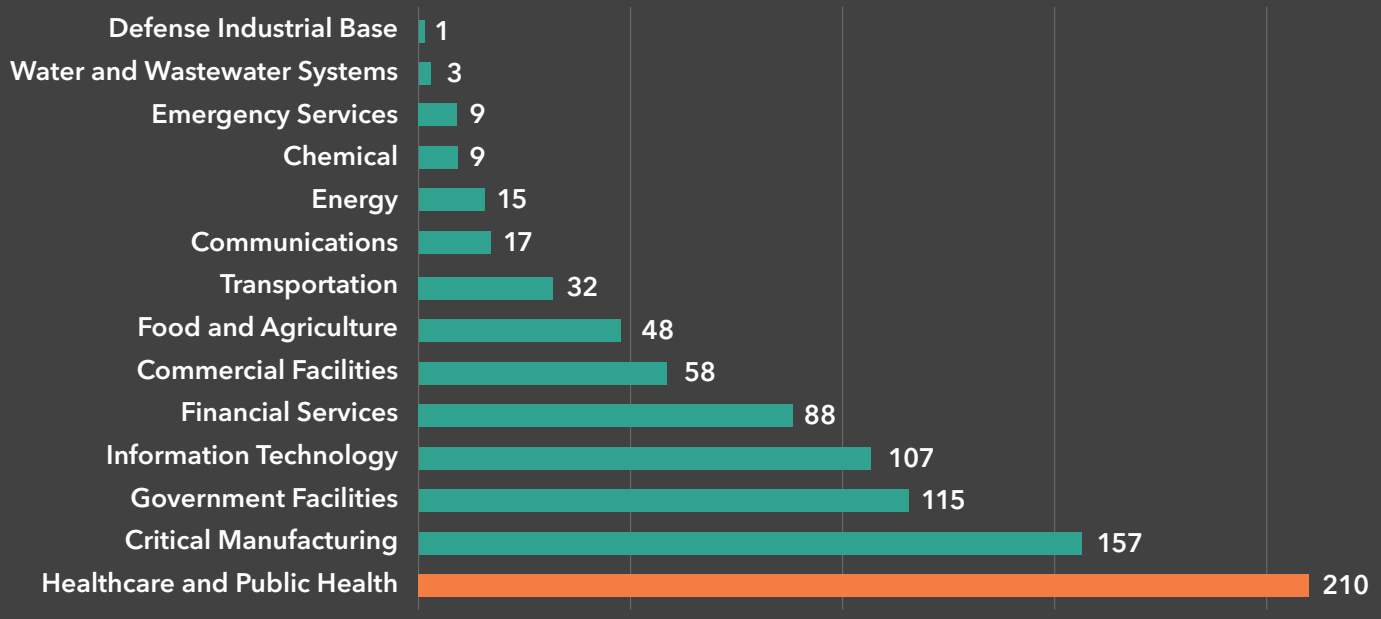
Or maybe the release of Senator Warner's policy options paper, **"Cybersecurity Is Patient Safety"** shed light on the major challenges faced by healthcare organizations. This paper sought recommendations and solutions for how to address these challenges effectively.

Perhaps it was merely the fact that healthcare continues to be the number one targeted critical infrastructure sector, accounting for 210 of the 870 documented ransomware attacks in 2022, according to the **Internet Crime Report for 2022**.

## Ransomware And Critical Infrastructure Sectors

The IC3 receivd 870 complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomwaree attack. Of the 16 critical infrastructure sectors, **IC3 reporting indicated 14 sectors had at least 1 member that fell victim to a ransomware attack in 2022**.

## Infrastructure Sectors Victimized By Ransomware



**Regardless of the reason for this newfound attention, considerable activity has taken place on Capitol Hill since the start of 2023. Here's a recap of the progress that's been made so far and what's on the horizon.**

## White House Cybersecurity Strategy

A clear indicator that cybersecurity has our government's full attention was the release of President Biden's **White House Cybersecurity Strategy** in March 2023. This strategy outlined five pillars:

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

The White House's cybersecurity strategy includes the establishment of cybersecurity standards, as outlined in Strategic Objective 1.1 of the plan: "Establish Cybersecurity Requirements to Support National Security and Public Safety," which emphasizes the need to establish cybersecurity regulations for safeguarding critical infrastructure.

Another notable section is Strategic Objective 3.2: "Drive the Development of Secure IoT Devices," which is aligned with the PATCH Act.

## PATCH Act

The healthcare sector's immediate focus within cybersecurity centers around the newly introduced **FDA requirement aimed at medical device security**. Known as the PATCH Act (Protecting and Transforming Cyber Healthcare), this rule had a soft roll out on March 29, 2023, and will be in full effect on October 1.

**10/1**

**The PATCH Act will be in full effect on October 1.**

PATCH requires device manufacturers to meet four new requirements before the FDA approves their new devices for market entry.

1. A plan must be submitted detailing how they will promptly identify and address vulnerabilities.
2. Procedures must be developed and maintained to ensure that devices are cybersecure, including regular updates and timely patches to address critical vulnerabilities.
3. A comprehensive "software bill of materials" (SBOM) must be provided.
4. Additional requirements specified by the Secretary must be complied with.

Although the PATCH Act may impact device costs as manufacturers strive to implement these new standards, its primary objective is to **prevent the influx of inadequately protected devices** into healthcare facilities and facilitate swift responses to identified risks. It is important to note however, that the rule does not fully address the concerns surrounding existing legacy devices, at least in the near term.

## Congressional Support For Healthcare Cybersecurity

Senator Warner has emerged as a leading advocate for tackling healthcare cybersecurity, consistently emphasizing its significance as **his top priority for 2023**. Currently, his team is actively evaluating over 60 responses to his policy option paper, including a comprehensive response from Fortified Health Security. This evaluation process is currently in the "refinement stage," underscoring the recognition of the intricate nature of this problem.

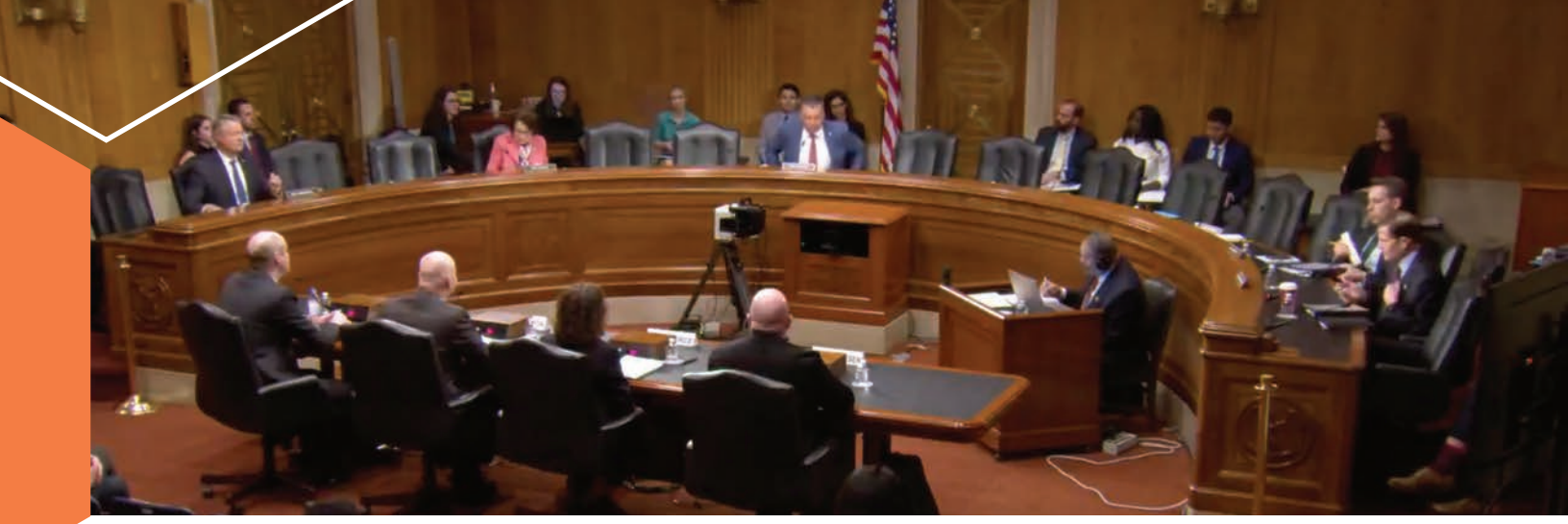
The evaluation has highlighted the complexity of the issue at hand, with various cabinet secretaries and federal agencies—sixteen in total—involved in healthcare and cybersecurity, each possessing crucial components of the solution. Given the multitude of stakeholders in shaping the policy roadmap, it is reasonable to anticipate the emergence of smaller bills that address specific aspects of the problem, rather than a singular comprehensive bill.

Despite the diverse array of issues and a lack of clear leadership, progress is being made. There is a growing momentum within the government towards finding viable solutions and addressing the pressing concerns within the healthcare cybersecurity landscape.

> **"The amount of damage that's been done is going to require standards."**

The intention to establish cybersecurity standards is evident from the statements made by Senator Warner and other lawmakers. While the exact timeline for implementing "minimum requirements" remains uncertain, language in the White House Cybersecurity Strategy, as well as by Senator Warner strongly suggests that serious consideration is being given to this matter.

As Senator Warner stated in an interview with **Politico**, "The amount of damage that's being done is going to require standards."



## Senate Hearing

**In March 2023, the Homeland Security and Government Affairs Committee held a Senate Hearing titled "In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector."**


Prompted by the **DC Healthlink breach**, which affected over 56,000 patients, the hearing brought together four expert witnesses, including **Kate Pierce from Fortified Health Security**, to provide insights into the current state of healthcare cybersecurity and offer recommendations for government support in enhancing our nation's cybersecurity posture.

During the committee hearing, **the expert witnesses gave testimony** on the challenges faced by healthcare organizations, the need for increased government assistance, and suggestions for improving overall cybersecurity practices in healthcare.

Subsequently, three significant documents were produced by the **Health Sector Coordinating Council (HSCC) Cybersecurity Working Groups (CWG)**, **the 405(d) program**, and **Health and Human Services (HHS)** outlining the current state of cybersecurity in healthcare and proposed next steps:

1. **Hospital Cyber Resiliency Initiative Landscape Analysis**
2. **Health Industry Cybersecurity Recommendations for Government Policy and Programs**
3. **Considerations for Prioritized Recognized Cybersecurity Practices for the Health Industry**

Collectively, these documents provided the government with a comprehensive view of current risks, active threats, and the healthcare sector's readiness in addressing cybersecurity challenges. Fortified also had the privilege of contributing to the creation of these documents, representing the voices of their customers.

## Rural Hospital Cybersecurity Enhancement Act

Following the submission of these three documents, Senators Hawley and Peters, both members of the Homeland Security and Government Affairs Committee, introduced a new bill titled the **Rural Hospital Cybersecurity Enhancement Act**. This legislation directly aligns with the testimony presented in the recent hearing.

The primary objective of this bill is to tackle the pressing issue of the cybersecurity workforce shortage in the United States, which currently stands at **nearly half a million workers**. The bill mandates that the Cybersecurity and Infrastructure Security Agency (CISA) develop a comprehensive strategy for enhancing the cybersecurity workforce in rural hospitals, as well as developing instructional materials and submitting annual reports with updates on the progress made.

Although this bill addresses one of the concerns raised during the hearing, it is reasonable to expect that future legislation will address several remaining concerns brought before the committee.

## Actionable Steps for the Future

While a positive step in the right direction, all these discussions around new cybersecurity standards and requirements for healthcare can feel overwhelming, especially considering the current financial uncertainties organizations are facing.

If these standards are imposed, meeting them will require time, effort, and resources, which might not currently be readily available for many organizations.

What has become abundantly clear is that funding is a crucial component for implementing these standards. The hope is that the government might offer incentives, grants, subsidies, or other resources to assist, but the specifics are yet to be determined.

As we wait on these policies and regulations to take shape, there are steps you can take to ensure your organization is ready:

- Read the three documents listed above under the Senate Hearing section and assess where your organization needs to improve its security posture
- Make plans to prioritize and tackle the areas that need attention
- Keep your leadership team in the loop about the upcoming changes to minimize any extra strain on your organization

By taking these proactive steps, you'll be laying the groundwork for readiness as the healthcare cybersecurity landscape evolves.

# Evading Detection: Unraveling Data Theft and Covert Tactics

**The healthcare industry has been increasingly targeted by cyber threats, and it's no secret that these attacks can have significant consequences.**

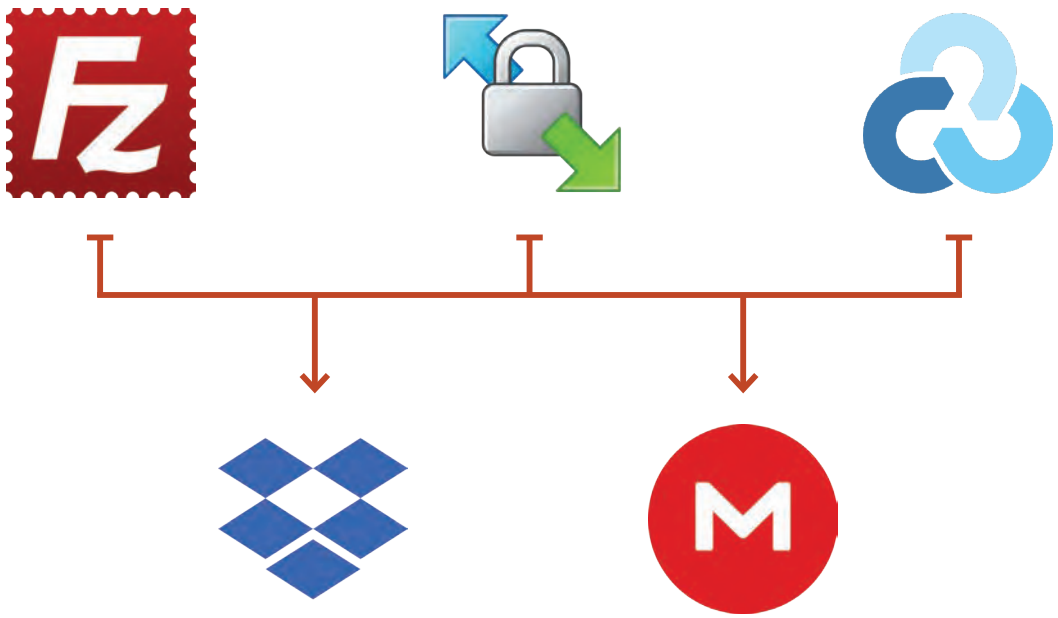
Two troubling trends that have emerged over the last few years have gained traction in recent months:

1. **Data theft using file transfer tools**
2. **"Living off the land" tactics**

## Data Theft

Cyber criminals are stealing data, including patient records, database files, office documents, etc., by using readily available tools such as FileZilla, Windows Secure Copy (WinSCP), and Rclone, among others.

These tools provide a secure connection, typically over SSH, to the attacker's chosen repository (often a cloud storage site like Dropbox or Mega).



A particularly alarming fact is that some of these tools can be installed without requiring administrative privileges or a full installation to the disk. They can be executed directly from memory or a flash drive, acting as portable applications. This tactic complicates the detection process, making it more challenging to identify suspicious activity at the application level.

### LIVING OFF THE LAND

When threat actors "live off the land," they employ various tactics within the operating system of an exploited machine to expand their reach and maintain a low profile.

Command line interfaces, PowerShell, and terminal sessions become their playground as they blend seamlessly with legitimate activities, making it difficult to detect their presence. To further conceal their actions, cybercriminals capitalize on weak or compromised Remote Desktop Protocol (RDP) credentials, effortlessly assimilating them into normal user behavior.

The strength of PowerShell scripting becomes their weapon of choice, allowing threat actors to execute commands, download additional payloads, and surreptitiously exfiltrate data through file transfer tools.

In their quest to conceal their malicious intent, threat actors manipulate trusted system files and hijack legitimate processes like run32.dll. By operating within the realm of legitimate activities and everyday behaviors, they're able to disguise their illicit activities.

To add insult to injury, threat actors employ scheduled tasks and cron jobs to automate their nefarious activities. These mechanisms ensure persistent unauthorized access within compromised systems, establishing a foothold for the attacker. Alternatively, they may serve as a "dead-man switch," ready to deploy ransomware at a moment's notice should the attacker's access be compromised.

The concept of living off the land extends beyond the initial entry operations. In fact, entire attack chains can be automated, leveraging these resources throughout the environment. The attackers seamlessly exploit available tools and functionalities, maximizing their efficiency and evading detection at every turn. Their adaptability and resourcefulness make them formidable adversaries in the realm of cybersecurity.

## How Threat Actors Gain Access

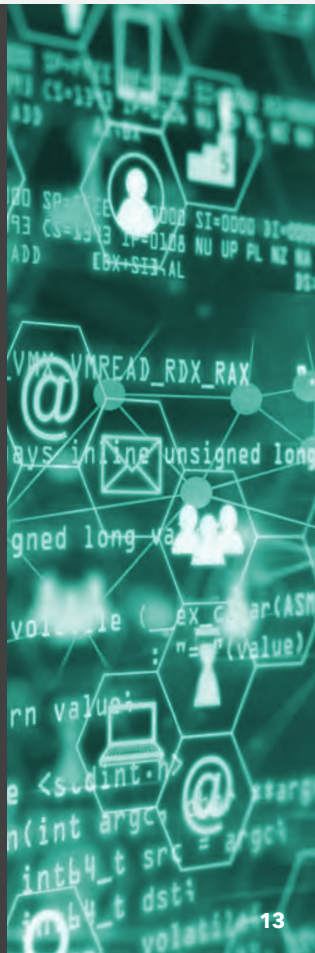
In their relentless pursuit of breaching networks, threat actors employ a range of tactics, including social engineering, password attacks, and vulnerability exploitation. Social engineering, in particular, is a crafty technique that often flies under the radar, relying on user observation and reporting for detection.

Password attacks, although equally stealthy, can be detected through vigilant monitoring of network and firewall logs.

Exploiting vulnerabilities presents another challenge in terms of detection, especially when the sole objective is gaining access. However, if a threat actor relies on malware during this stage, reputable endpoint technologies can come to the rescue by thwarting the attack vector.

Once inside a compromised system, threat actors leverage the accessible features within the operating system to extend their visibility and access.

Armed with this knowledge, threat actors may launch further password attacks against the entire list or intensify their social engineering efforts, casting a wider net in the hopes of ensnaring more victims.



## What to Know and Do

It's imperative to remain vigilant against these tactics and adopt robust security measures to mitigate the risks posed by cyber threats. To protect your organization from these threats, consider implementing the following measures:

- **Principle of least privilege:** Limit remote access functionality to only those users who require it and restrict access to specific services within those resources.
- **Access and authentication:** Implement **multifactor authentication** (MFA) across all systems, especially for internet-facing resources. Encourage the use of complex passwords or passphrases and consider obfuscating usernames to prevent easy identification.
- **Endpoint protection:** Traditional antivirus solutions may no longer be sufficient. Explore advanced endpoint protection tools like SentinelOne and Cybereason that offer enhanced features such as system isolation, behavioral analysis, and comprehensive response capabilities.
- **Logging:** Ensure comprehensive logging across your systems and work closely with your Security Information and Event Management (SIEM) provider to aggregate and monitor relevant logs. Consider adopting an "XDR" (Extended Detection & Response) approach that combines network and system logs with endpoint intelligence for better visibility and correlation.
- **Stringent firewall rules:** Restrict outbound SSH connections and file transfer capabilities at the firewall to explicitly known and justified purposes and destinations. By doing so, you make it challenging for threat actors to upload stolen data. Regularly test your firewall accuracy by uploading a known-sized object and confirming the accuracy of related log entries.

By staying proactive and adopting a multi-layered defense strategy, you'll be better positioned to protect your healthcare organizations, valuable data, and mitigate the risks associated with these covert cyber threats.

# ChatGPT in Healthcare: Insights from the Experts

**To say that artificial intelligence—ChatGPT in particular—is a hot topic of 2023 is like saying airplanes revolutionized the way we travel in the 20th century.**

While much of the enthusiasm (and agitation) around ChatGPT has been focused on its ability to help with crafting pithy social posts, searching for answers, and writing Excel formulas, there's growing concern among cybersecurity professionals that ChatGPT can be used for more nefarious purposes.

We reached out to experts in our cybersecurity community to get their take on how ChatGPT could impact security within healthcare organizations.

"Generative AI, like ChatGPT, represents a remarkable technological leap. But with great power comes great responsibility, especially in the realm of healthcare cybersecurity. Just as hospitals and health systems evaluate the benefits and risks of medical tools and technology, so should they evaluate how open-source AI is used within their organization. There are still a lot of unknowns, including where all that information goes and how easy it is for someone to get access to it. In short, proceed with caution and put the right evaluation protocols in place."

- **Scott E. Augenbaum**, Cybercrime Keynote Speaker | Retired FBI Supervisory Special Agent of the Cyber Division | Author

"The reality is, there is currently no way to use ChatGPT with protected health information (PHI) while maintaining HIPAA compliance. Chatbots, unless explicitly stated otherwise, are not HIPAA-compliant and require additional measures to secure PHI and related data. Regardless of anonymity measures, chatbots inherently reveal user information, posing risks of identification and tracking.

It's crucial to remember that Chat GPT is a third-party entity, akin to divulging information to a stranger at a pub. While they claim anonymization, it may not always be reliable. Unauthorized disclosure of confidential information to Chat GPT can breach NDAs and result in severe penalties or dismissal. To avoid such breaches, review your NDA and internal policies, consult legal counsel or privacy officers, and ensure removal or alteration of confidential data before engaging with Chat GPT.

In addition, due to security and privacy concerns, blocking is not an ideal approach because, sooner or later, we'll have to live and deal with it. However, I suggest each organization develop policy and controls around how / when ChatGPT can be leveraged, with required logical and technical controls."

- **Raj Patel,** Virtual Information Security Officer, Fortified Health Security (insights based on social media and internet research)

"There are still so many unknowns about the potential impact of ChatGPT and other AI when it comes to healthcare cybersecurity. Security vendors have been touting the advancements of AI for years, so it's interesting to see how it's all starting to play out in real-time. Personally, I was curious what ChatGPT would say on the matter, so I went straight to the source.

The tool stated that it can have a significant impact on healthcare cybersecurity in several ways including: threat detection and response analysis/automation, security awareness training simulations, vulnerability management analysis/remediation, patient education, and support for their 'cyber hygiene' awareness, and data privacy compliance to help monitor data access flows/requests.

While that remains to be seen, the ending of the ChatGPT response is what I found to be the most insightful:

'While ChatGPT can provide valuable support in healthcare cybersecurity, it is not a substitute for comprehensive cybersecurity measures. Human expertise, regular security audits, and other specialized tools are still essential components of a robust cybersecurity strategy in healthcare organizations.'"

- **Robert C. Swaskoski,** CISO at Heritage Valley Health System

"As the promise of generative AI in healthcare is now a major focus for hospitals and health systems, and every third-party technology provider that sells to us, we must also take note of the urgent warnings issued by those technology companies who helped develop generative AI and the brightest minds in that field. Never before have we seen Big Tech and academia align and call for government regulation on a new technology, with many experts formally calling for a moratorium on the further development and distribution of AI.

Why? As many of the experts in the field have stated, they do not fully understand how these artificial neural networks arrive at their conclusions. In fact, the results may be 'authoritatively incorrect' and biased. What's more is that AI may present a privacy and security risk to our most sensitive data. Some of the leading experts even warn that uncontrolled AI will pose an existential threat to humanity.

As with all technology, we must first understand how it truly functions to identify and control risk. No doubt, generative AI presents great hope to improve patient outcomes and potentially find cures for the leading causes of illness and death. But before we inextricably integrate AI into our networks, we must understand the risks as well as the rewards."

- **John Riggi,** National Advisor for Cybersecurity and Risk, American Hospital Association)

"AI is a force multiplier, but my two primary concerns surround the protection of confidential information and fraud. As users enter confidential information into something like ChatGPT, they lose control of that information. No one really knows where it will go or how it can be used. Losing control of PHI could be considered a breach for HIPAA Covered Entities.

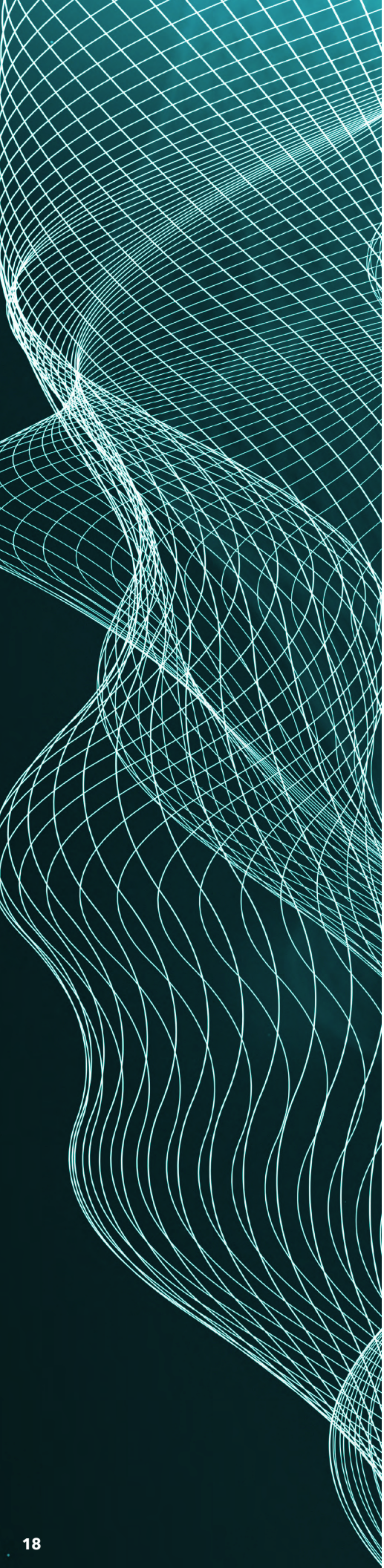
> **To me, fraud is an even bigger threat as it affects real people. The days of training nurses and doctors to recognize a phishing email using poor grammar or bad spelling are over. Now, anyone can create a spear phishing email using proper syntax, style, and desired tone.**

Worse, AI allows the use of deepfakes for sextortion and societal manipulation. In a world where the majority of people will not read beyond a headline or graphic, the damage that could be done by a deepfake video or photo could lead to societal instability, political manipulation, and even worse. I don't think that is an overstatement!

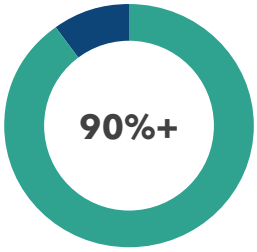
On a micro level, it is easier now to defraud regular people by creating interactive, synthetic voices from audio samples. Teach your employees to recognize vishing attempts. Don't rely on CallerID. If you are a CEO, consider implementing a 'safe word' and sharing it with your CFO or executive team to use in case of a true emergency or in an instance where money needs to be transferred by wire."

- **Don Kelly,** Senior Virtual Information Security Officer | Manager, VISP Program, Fortified Health Security

**Experts clearly recognize the potential benefits of ChatGPT. However, they also caution against risks of using it in a healthcare environment, such as unauthorized data disclosure and fraud. The overall consensus is the need for careful evaluation, policies, and controls to ensure responsible and secure implementation, and prioritizing human expertise and comprehensive cybersecurity measures.**



# Exploring the Strengths of Risk-Based Identity Alerting




In cybersecurity, phishing attacks are as ubiquitous as hashtags in social media posts.

**Phishing incidents have become the go-to starting point for more than 90% of all cyberattacks, and the numbers keep rising. Just last year, there was an 87% spike in attacks across different industries, and a whopping 356% surge in advanced phishing attacks.**

To combat the barrage of increasingly sophisticated phishing attempts, risk-based identity alerting is gaining traction within hospitals and health systems.

## What is Risk-Based Identity Alerting?

Risk-based identity alerting monitors user activity based on anticipated actions, triggering multi-factor authentication (MFA), halting access, or alerting the IT team when activities stray into unexpected territories based on the user's profile or when unconventional commands are used.

In an effort to deter unauthorized access to a system, IT departments enforce stringent password requirements, such as longer passwords incorporating a combination of uppercase and lowercase letters, numbers, and symbols. Many also require a different login for different systems or require frequent password changes. However, once a user has successfully logged in, they obtain unrestricted access to any network resources within their authorized privileges.

As phishing attacks continue to rise and attackers get better at it, relying solely on the login process as the final line of defense is no longer sufficient. It's crucial to consider the actions users take once they have successfully logged in to the network.

While it's expected for a clinician to access the Electronic Health Record (EHR), certain activities like running a PowerShell command should raise a huge red flag. Once hackers infiltrate an IT system, their initial steps typically involve running PowerShell or using a tool to map the domain to identify vulnerable areas and privileged accounts.

## Common Ways Healthcare Organizations Protect User Accounts

### Active Directory (AD)

In a hospital environment, Active Directory is frequently used to manage permissions and access privileges for software and network resources. Administrators rely on AD to control user authentication, assign appropriate access levels, and maintain the security of critical systems and data within the hospital network.

However, many healthcare systems often lack comprehensive awareness and effective management of their Active Directory (AD) environments. It's common to uncover service accounts and privileged user accounts that have not had their passwords updated in years, logins for employees who have long since departed, permissions granted to individuals that may not be necessary, and a lack of a centralized and dependable user and permission registry that IT staff can fully rely on.

While it is possible to clean up the Active Directory, that takes time and resources that most IT departments don't have.

### Multi-Factor Authentication (MFA)

**Multi-factor authentication** is a fantastic tool for assisting in verifying that the correct user is accessing the correct resource, but it doesn't help solve the issues with dormant users or ancient passwords. It's like wrapping another security control over an environment that no one really understands in the first place.

### User and Entity Behavior Analytics (UEBA)

Many healthcare systems implement user and entity behavior analytics (UEBA) solutions, leveraging advanced algorithms and machine learning to identify irregularities in both user and machine behavior. While UEBA software can determine the "what" of an anomaly, it can't answer the "why" questions.

## How Risk-Based Identity Alerting Adds an Extra Layer of Protection

Risk-based identity alerting plays a critical role in enhancing security by mapping user accounts and assigning risk levels based on user type, accessed resources, and recent behaviors. This approach provides valuable insights into anomalous behavior, empowering IT staff with clearer information to address the "why" behind suspicious activities.

Through risk-based identity alerting, certain risk levels may automatically trigger responses like multi-factor authentication (MFA) for additional verification or account lockouts to mitigate potential threats.

In the context of hospitals and health systems, risk-based identity alerting is especially useful to those with a "messy" Active Directory environment, a half-hearted MFA implementation, and noisy UEBA alerts, as it gives the visibility to plan any necessary improvements while offering protection against threats along the road to maturity.

# 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 healthc are 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*.

**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.

**RAJ PATEL**
*Virtual Information Security Officer*
Fortified Health Security

Raj has over 25 years of experience in IT and healthcare cybersecurity management. Raj has extensive expertise in developing cybersecurity strategies and architecture to protect organizations from external and internal cyber attacks and ensure the privacy, security, and availability of healthcare services. His background spans various industries, including hardware manufacturing software development, utilities, and healthcare sectors.

**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.

**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.

**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.

**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.

**ROBERT C. SWASKOSKI**
*CISO*
Heritage Valley Health System

Robert (Bob) Swaskoski currently serves as the Chief Information Security Officer for Heritage Valley Health System, Inc. In his capacity as CISO, Bob is responsible for overall security strategy as well as managing the implementation of cybersecurity policies and programs to reduce risk and protect Heritage Valley's information assets. His experience in Information Technology spans a 35-year career and includes leadership positions in computer solution sales, project management, consulting, and software development in both the retail and healthcare industries. Bob views himself as a "business entrepreneur with an appreciation for technology" and this insight has enabled him to consistently improve his customer experiences while growing revenue and managing costs. Bob holds a B.S. in Business and Information Technology from Duquesne University and is a member of InfraGard.

**SCOTT E. AUGENBAUM**
*Cybercrime Prevention Trainer, Author & Keynote Speaker*

Scott Augenbaum is a retired FBI Supervisory Special Agent for the CyberCrime Fraud Division in the United States, as well as a cybercrime prevention trainer, speaker, and author of the best-selling book "The Secret to Cyber Security" (a simple plan to protect your family and business from cybercrime).

He responded to thousands of cybercrime incidents during his three decades with the FBI and speaks on how to defend against cyber threats and vulnerabilities. He has appeared on popular news programs such as The Dr Phil Show, News Nation, Fox & Friends, CRN, News Nation, WSMV, News Channel 5, MSNBC, and Bloomberg, as well as the BBC and other international outlets.

**JOHN RIGGI**
*National Advisor for Cybersecurity and Risk*
American Hospital Association

John Riggi, a 30-year highly decorated veteran of the FBI, serves as the first national advisor for cybersecurity and risk for the American Hospital Association. In this role, he serves as a trusted advisor to the leadership of nation's hospitals and health systems. John is a prominent national advocate on healthcare cyber policy and legislative issues – including providing testimony and briefings to Congress which assisted in the passage of PL 116-321, which provides regulatory relief for HIPAA covered victims of cyber attacks. In 2021, John's prominent advocacy encouraged the government to raise the investigative priority level of ransomware attacks to equal that of terrorist attacks. John works closely with healthcare victims of cyber ransomware attacks during and post attack.

While at the FBI, John served as a representative to the White House Cyber Response Group, a Senior representative to the CIA and on the NY FBI SWAT team for eight years. He is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the CIA's George H.W. Bush Award for Excellence in Counterterrorism, the CIAs highest counterterrorism award.

# 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.

# Sources


[1] Source: https://techcrunch.com/2023/05/04/millions-patients-data-stolen-fortra/

[2] Source: https://techcrunch.com/2023/03/24/fortra-goanywhere-clop-ransomware/

[3] Source: https://www.cisa.gov/sbom

[4] Source: https://healthitsecurity.com/news/healthcare-sector-spearheads-sbom-adoption-to-support-cybersecurity

[5] Source: https://www.healthcaredive.com/news/commonspirit-third-quarter-operating-loss-job-cuts/650364/

[6] Source: https://www.healthcaredive.com/news/commonspirit-third-quarter-operating-loss-job-cuts/650364/

[7] Source: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[8] Source: https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf

[9] Source: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[10] Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[11] Source: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section

[12] Source: https://www.fiercebiotech.com/medtech/under-new-law-fda-submissions-must-prove-medical-devices-meet-cybersecurity-standards

[13] Source: https://www.washingtonpost.com/politics/2023/01/25/sen-warner-cyber-priority-this-year-is-health-care/

[14] Source: https://www.politico.com/newsletters/future-pulse/2023/01/17/health-cybersecurity-rules-are-on-the-table-00078055

[15] Source: https://oversight.house.gov/wp-content/uploads/2023/04/Mila-Kofman-Written-Testimony-April-19-2023.pdf

[16] Source: https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Pierce-2023-03-16.pdf

[17] Source: https://www.hsgac.senate.gov/hearings/in-need-of-a-checkup-examining-the-cybersecurity-risks-to-the-healthcare-sector/

[18] Source: https://healthsectorcouncil.org/

[19] Source: https://405d.hhs.gov/

[20] Source: https://www.hhs.gov/

[21] Source: https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

[22] Source: https://healthsectorcouncil.org/wp-content/uploads/2023/04/HEALTH-INDUSTRY-CYBERSECURITY-RECOMMENDATIONS-FOR-GOVERNMENT-POLICY-AND-PROGRAMS.pdf

[23] Source: https://healthsectorcouncil.org/wp-content/uploads/2023/06/Considerations-for-Prioritized-Recognized-Cybersecurity-Practices.pdf

[24] Source: https://www.hawley.senate.gov/hawley-peters-introduce-bill-improve-and-protect-rural-hospitals-cybersecurity

[25] Source: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[26] Source: https://fortifiedhealthsecurity.com/blog/single-sign-on-vs-mfa-do-you-know-the-difference/

[27] Source: https://www.cisa.gov/stopransomware/general-information

[28] Source: https://www.securitymagazine.com/articles/99435-report-advanced-phishing-attacks-grew-356-in-2022

[29] Source: https://fortifiedhealthsecurity.com/blog/single-sign-on-vs-mfa-do-you-know-the-difference/

# Fortified HEALTH SECURITY



www.fortifiedhealthsecurity.com

1 (615) 600-4002

2550 Meridian Blvd, Suite 190
Franklin, TN 37067