Fortified
HEALTH SECURITY

# 2021 Mid-Year Horizon Report

## The State of Cybersecurity in Healthcare

# CEO's Message

As we look back over the past year, it was hard to believe that businesses could simply shut down and close for months. Travel and hospitality industries halted. Manufacturing and transportation industries disrupted. But one thing was clear – the healthcare industry could not close; it could not stop providing care, no matter the risk.

Now as the healthcare industry gets some breathing room from the pandemic, another one is surging – cyber attacks. Like the pandemic, these attacks have the ability to prevent hospitals from providing care to patients. Malicious actors are targeting the healthcare industry specifically for that reason.

We have entered a new era with the criminals behind these attacks. This year we have seen ransomware-as-a-service become a normality in the cybercrime community, with cyber gangs being supported by nation-state actors. Not only are these gangs committing the crimes, but they are offering support to other thieves to orchestrate more attacks.

Their attacks have caused sizeable damage in all industries. The sophistication and severity of attacks on healthcare has pushed the average cost of a breach to more than $7 million per incident, a 10% increase in just one year.[1] Further, these attacks affect not just the bottom line but severely hamper patient care and the brand reputation. Lawsuits are being filed by patients who were prevented from receiving care during a cyber incident with increasing regularity. These increasing costs have also caused underwriters of cyber insurance to rethink policy renewals and require attestations around the deployment of certain cybersecurity tools in order to maintain cyber insurance coverage.

The attacks on our nation's critical infrastructures which includes our hospital systems, has resulted in government agencies showing a renewed focus on cybersecurity. This has helped move cybersecurity to the forefront of many boardroom discussions. We, as healthcare leaders, must seize this opportunity to educate and inform stakeholders on the current cybersecurity threat landscape and the actions needed to combat these attacks.

Technologies and tools being in place are not a guarantee that a hospital is secure from these cyber attacks. Employees are often targeted by attackers as a way to bypass technical security controls. Infusing cybersecurity into the mindset of all employees is a cultural change which needs to be prioritized and adopted throughout the entire organization. Leaders must realize that employees are on the frontline of these sophisticated attacks, and it is an organizational responsibility to be diligent in our efforts to protect patients and patient data.

To combat these gangs and their criminal activity, it is important that we also adopt a collaborative mentality and share ideas freely. Developing a cyber aware culture is a necessity within the hospital and health system. Additionally, it is just as important to leverage other ecosystem resources to stay informed of emerging threats, listen to lessons learned from our peers and to discover additional tips used by other security professionals to stave off the bad actors to protect their environments, patients, and data.

My hope is that the Horizon Report builds awareness about the cybersecurity landscape in healthcare and provides valuable insight for your program. We welcome your feedback and perspective at: horizonreport@fortifiedhealthsecurity.com. Enjoy.

Regards,

Dan L. Dodson, CEO
Fortified Health Security

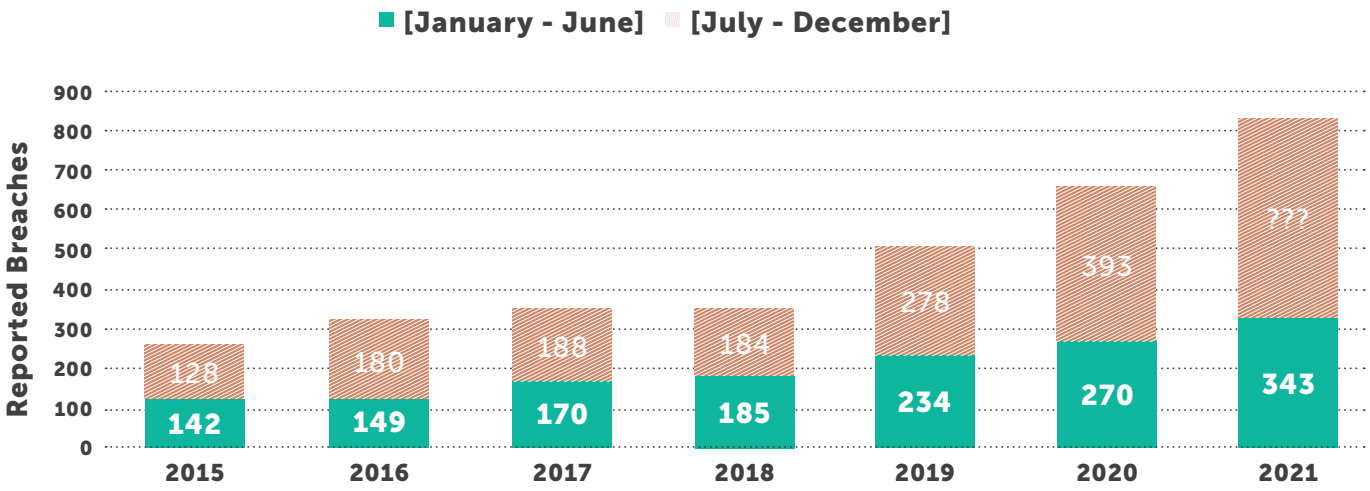
[1] Source: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

# 2021 Mid-Year in Review

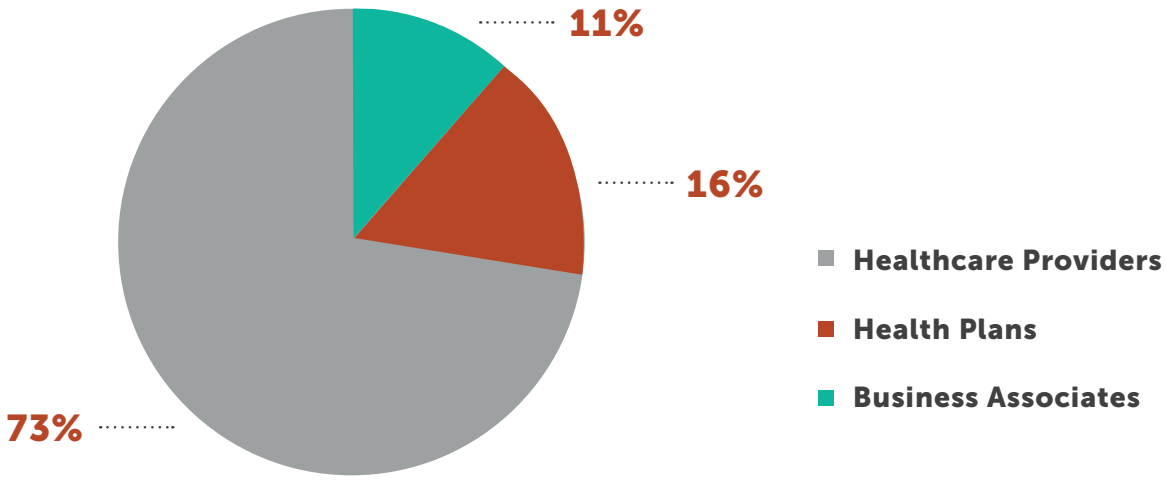
The US healthcare market continues to face an increase in cybersecurity threats from bad actors, and the first half of 2021 has shown that the increase remains in double-digit territory. Hackers and cyber criminals kept up their malicious efforts throughout the pandemic, causing well-known and widespread breaches and cyberattacks across all industries, but especially the healthcare industry.

During the first half of 2021, the number of breaches reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR)[2] numbered 343. That equates to a 27% year-over-year increase between mid-year 2020 and 2021, compared to a 15% increase between mid-year 2019 and 2020. Healthcare providers continue to account for the most breaches 73% of the total, with health plans accounting for 16%, and business associates, 11%.

## Number of Breaches Reported



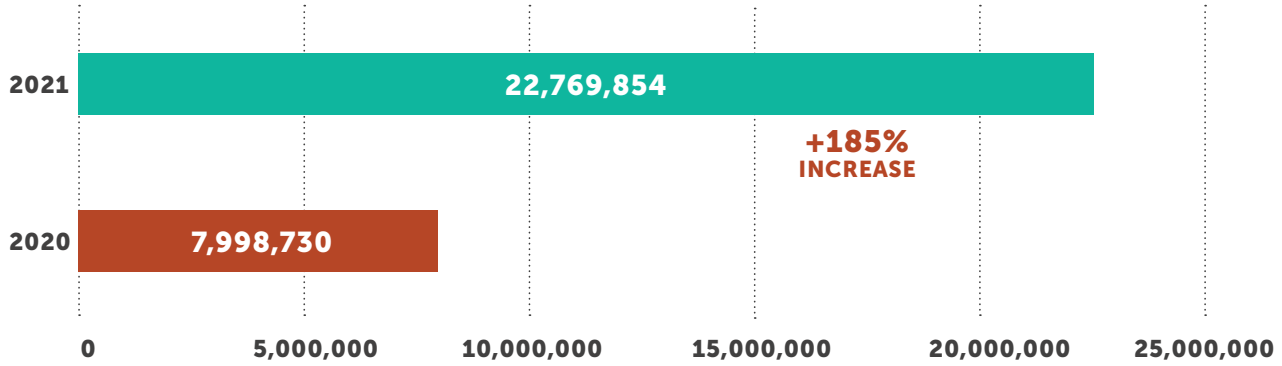

## Those Affected by Breaches




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

The total number of individuals affected skyrocketed more than 185%, from 7.9 million in the first six months of 2020 to 22.7 million affected in the first six months of 2021. However, just five breaches accounted for more than 50% of all affected, 11.13 million total. An anesthesia practice and a grocery store chain that has pharmacies/clinics combined for 2.73 million. One health plan reported a breach of 3.5 million records and two business associates reported 4.9 million impacted.

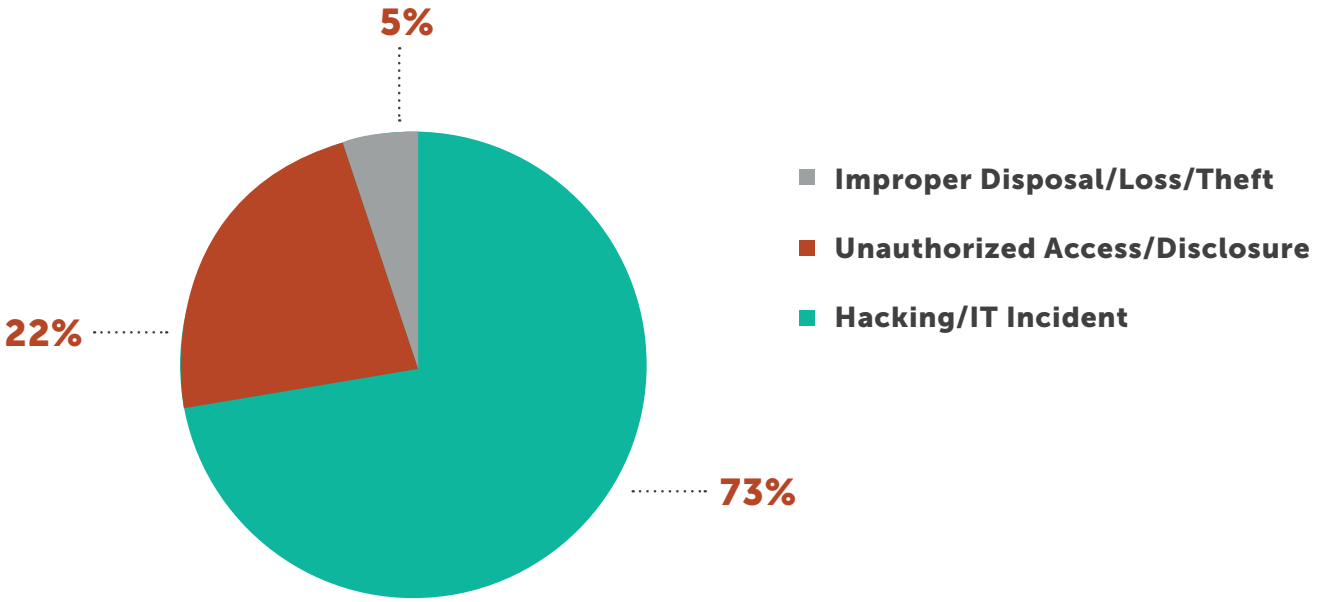
## Number of Individuals Affected




**Individuals affected - January through June**

It is interesting to note that malicious attacks were the No. 1 cause of breaches for the fifth consecutive year, and for three years running, malicious attacks accounted for 73% of all breaches. Unauthorized access/disclosure accounted for another 22%, with much smaller numbers of thefts, losses, and improper disposals. Healthcare organizations have literally hundreds of electronic entry points into their data networks, everything from EHRs, radiology and lab systems, to admission, discharge and transfer systems, to supply chain ordering and internet-enabled medical devices — and any one of these could be the Achilles' heel exploited by a bad actor.

## Cause of Breaches



The pandemic sent most non-patient-facing healthcare workers home, as they traded the hospital or medical office for a spare bedroom or the kitchen table. The prevalence of remote working vastly expanded the attack surface that healthcare cybersecurity teams had to protect as data moved beyond the four walls of the hospital and into employee's homes throughout the community.

The continuing issue of worker inattention underscores the importance of an effective employee security training and awareness program. Just as your organization should conduct periodic training on HIPAA privacy and security, make email training and cybersecurity awareness a priority for your organization to help reduce the frequency of successful phishing attacks.

Reputational risk can be quite high for organizations that suffer a breach, but healthcare faces significantly higher risks due to the sensitive nature of healthcare data.

Higher-profile ransomware attacks that have occurred in healthcare and non-healthcare settings have caught the attention of public and federal authorities. Reputational risk can be quite high for organizations that suffer a breach, but healthcare organizations face significantly higher risks due to the sensitive nature of healthcare data. Healthcare organizations must remain vigilant to make sure their technology infrastructure remains secure. They must also honestly assess whether internal cybersecurity resources are sufficient to keep their organizations and patient data safe.

**Pause to Consider**

1. How has your potential attack surface changed because of the pandemic?
2. What actions are you taking to combat the emerging threat landscape?
3. Are you confident that the cybersecurity training provided to your employees is adequate?

# Notable Attacks & the Criminals Behind Them

The attacks that gained the most notoriety in 2020 were the supply chain hack of SolarWinds, a software developer for businesses to help manage their networks, systems and information technology infrastructure, and the hack of Blackbaud, a cloud computing provider. In both instances, their attackers succeeded in infiltrating their systems and were able to move laterally into other companies, organizations and government agencies. These movements and additional breaches from a single source provided a catalyst that brought hyper focused awareness by government agencies, including the FBI, Department of Health and Human Services (HHS) and Department of Homeland Security (DHS) to combat cybercrime and treat it as a threat to national security.

The fallout from the SolarWinds and Blackbaud hacks continues to reverberate throughout the economy, including the healthcare industry. SolarWinds alone potentially affected 18,000 companies, including more than 400 of the Fortune 500 and the U.S. Department of Homeland Security. Blackbaud's breach hit healthcare particularly hard, affecting an estimated 100 organizations.

Organizations must remain vigilant not only of their own networks but as to those vendors and organizations granted intentional access to their networks because every connection to a technology or among technologies and each user ID and password is a potential entry point for malware that can lead to a cyberattack or data breach.

So, what is a healthcare organization to do? The first step to deterring attacks is understanding your organization's attack surface and risk tolerance. Then building a defense plan from there. Taking a close examination of significant breaches like Blackbaud and SolarWinds will increase your understanding of how such incidents can occur, and the motivation of the groups behind these attacks.

The first step to deterring attacks is understanding your organization's attack surface and risk tolerance. Then building a defense plan from there.

## Vendor Breach Hits Healthcare Hard

Due to Blackbaud, 2020 marked the second consecutive year that a third-party vendor caused the year's largest healthcare data breach. The breach began in February 2020, indicating that the pandemic was not a primary factor. However, the fundamental shift of workers to remote settings that started with the near-universal national shutdown in March amplified potential vulnerabilities, as did the move toward more outsourced technologies to power modern healthcare environments.

Based in South Carolina, Blackbaud provides "cloud software, services, expertise, and data intelligence that empower and connect people to drive impact for social good," according to the company website. That "social good" includes hospitals and health systems impacted by the breach.

The specific origins of the Blackbaud breach remain unclear, but cybercriminals infiltrated its IT systems in February 2020 and copied sensitive information that included not only full names, dates of birth, and email addresses, but Social Security numbers, usernames and passwords, and bank and credit card information. Certain demographic information can be used to create false identities, while more specific information like banking details can be used in sophisticated phishing attempts with emails that purport to come from the target's bank or credit card company.

Blackbaud internal cybersecurity staff noticed the breach three months later and immediately took steps to expel the attackers from their network. While these actions kept the attackers from encrypting Blackbaud data and seizing systems, the criminals still successfully negotiated a ransom for the stolen files, promising to destroy them upon payment. Blackbaud hired experts to monitor the dark web in case the information was sold, but say they have not seen any evidence to suggest it.

As a result of the breach, Blackbaud faces nearly two dozen lawsuits, including one filed in the Western District of Washington that alleges, "Had Defendants properly monitored their networks, security, and communications, they would have prevented the data breach or would have discovered it sooner." [3]

## SolarWinds Hack Raises Profile of Cybersecurity

The SolarWinds breach is particularly heinous for the length of time between intrusion and detection and the ubiquitous nature of the software, a network and applications monitoring platform that is used by nearly 18,000 companies. Hackers are believed to have gained entry through a successful phishing expedition, then wormed their way into the company's software build environment to place malicious code amid legitimate software that was pushed out to customers in the form of regular updates.

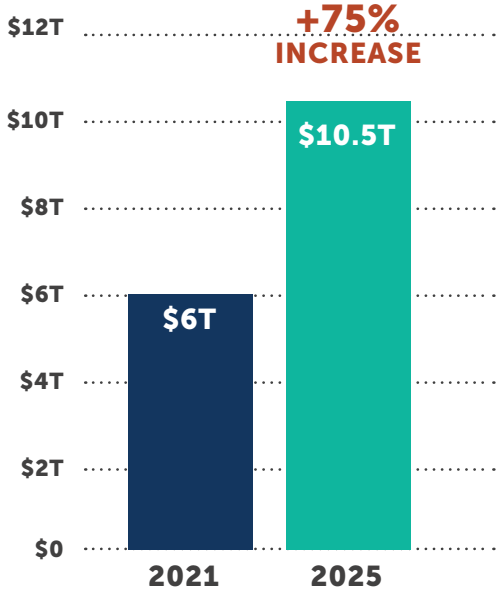
An extensive forensic audit discovered the hack's origins in January 2019, but the attack was not discovered until December 2020, an egregious amount of time — especially for a software vendor. The breach was not discovered by SolarWinds but by an affected client, a cybersecurity firm that uses SolarWinds technology to monitor customer networks.

## Ransomware-As-A-Service

Cybercrime is expected to inflict $6 trillion in global damages this year, a figure predicted to climb to $10.5 trillion by 2025. If cybercrime was a country, it would be the world's third-largest economy, trailing only the United States and China.[4] More than nine in ten U.S. companies have suffered a breach in the past year due to a supply chain weakness.[5] State-sponsored hackers in Russia, China, North Korea, and others are increasingly responsible for many of these sophisticated attacks.

**Magnitude of Cybercrime**

*Expected Global Damages Per Year*




[3] Source: https://healthitsecurity.com/news/blackbaud-confirms-hackers-stole-some-ssns-as-lawsuits-increase
[4] Source: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[5] Source: https://www.scmagazine.com/home/security-news/supply-chain-weak-security-link-for-92-percent-of-u-s-companies/

In a June 2021 report, the *Wall Street Journal* tracked the most disruptive attacks to one group: a notorious gang of Eastern European cybercriminals once called the "Business Club." According to threat analysts and former law-enforcement officials who closely follow Eastern European cybercrime operations, this group has ties to Russian government security services.[6] This group is also known as Ryuk, after its signature software. They are said to be responsible for 203 million U.S. ransomware attacks in 2020 and have targeted at least 235 hospitals.

Although the cybercrime gang known as DarkSide, said to be behind the Colonial Pipeline hack, claims it will not hack hospitals, nursing homes, schools and government targets, it is the notion of "professionalizing" the cybercrime industry that is alarming. The group has developed and marketed ransomware hacking tools to sell to other criminals who then carry out attacks leveraging those tools.[7] DarkSide claims their hacks are not political; both DarkSide and Ryuk gangs are motivated by money.

With cybercriminal groups working as a business, selling tools and techniques and announcing a target list of 400 hospitals in the US and UK, in October 2020 the FBI took a proactive measure to release an alert about an impending attack. Although HHS confirmed that 250 facilities in the US were affected by the attack in October, they believe that based on the early alerts, many hospitals took strong measures to minimize the exposure. Federal investigators concluded that Ryuk was behind the attack, which was unprecedented in terms of scale and sophistication. Ryuk was reportedly responsible for 75% of the attacks on the US healthcare sector in October 2020.[8]

## Federal Government Attention

If there is a silver lining to the SolarWinds breach, it is the increased profile of cyberattacks and emerging federal government efforts to increase security protocols. While ransomware attacks impact all sectors, the federal government is particularly concerned about the impact on the healthcare industry. These types of attacks have shut down hospitals, prevented access to lifesaving equipment and directly impacted the ability for hospitals to care for patients.

In a statement released after their testimony before the Senate Homeland Security Committee in December 2020, the American Hospital Association (AHA) "acknowledges and commends the U.S. government's efforts to share timely and actionable cyber-threat intelligence. However, relying on victimized organizations to individually defend themselves against these attacks is not the solution to this national strategic threat." [9]

Even with federal government intervention, the healthcare industry must remain proactive. As the AHA suggests, the healthcare industry needs to work together in a coordinated way to share information across the healthcare ecosystem.

### Pause to Consider

1. What procedures does your organization have in place to detect and protect against similar attacks?
2. Does your organization verify the security certificates and credentials of its IT supply chain partners?
3. When researching IT vendors, where does security rank among selection criteria?
4. Do you share experiences and lessons learned with other healthcare organizations?

[6] Source: https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215
[7] Source: https://www.cnbc.com/2021/05/10/hacking-group-darkside-reportedly-responsible-for-colonial-pipeline-shutdown.html
[8] Source: https://www.hhs.gov/sites/default/files/ryuk-variants.pdf
[9] Source: https://www.aha.org/advisory/2021-05-21-fbi-issues-conti-ransomware-alert-high-impact-global-attacks-persist-against

# The Human Element of a Cyberattack

Humans often are the weakest link in the cybersecurity chain, with curiosity or inattention taking the place of vigilance and caution in the face of an ever-increasing number of phishing (email), voicemail phishing (vishing), texts (smishing), and fraudulent websites (pharming) attacks. The dramatic increase in overall attacks so far this year compared to 2020 should serve as a stark reminder that organizations must proactively monitor both their IT networks and their personnel. Furthermore, this validates that many healthcare organizations still struggle with executing basic security fundamentals like patching and remediating gaps, which leaves them vulnerable.

The FBI Internet Crime Complaint Center (IC3) received over 790,000 complaints during 2020, with reported losses of $4.1 billion. That is a 69% increase over the number of complaints filed during the previous year. In terms of sheer numbers, phishing, vishing, smishing, and pharming account for 30% of all attacks and double the number of attacks reported in 2019. In terms of dollar losses, however, business email compromise (BEC) and email account compromise (EAC) attacks are the most costly, with 19,000 complaints and $1.8 billion in losses. [10]

The IC3 report notes that BEC/EAC attacks are growing in sophistication. A decade ago, email scams generally started with the hacking or spoofing of C-suite email accounts, followed by fraudulent emails to accounts payable staff requesting wire payments to fraudulent locations. Much like a virus, these scams have evolved over time to include compromise of personal and vendor emails, spoofed attorney email accounts, W-2 requests and requests for gift cards.

## Emerging Types of Threats

Vishing attacks were first reported in December 2019 and have proliferated in number, type and complexity since then. Targets are phone users on VoIP platforms used by large, global companies. The latest threat combines vishing with pharming, calling workers and coercing them to log into a fraudulent website so criminals can capture usernames and passwords. From there, attackers can access a company's network and inflict further damage. Other vishing threats include a massive mining campaign to gather login credentials for later attacks and exploiting legacy voicemail technology to ensnare remote healthcare workers.[11]

Hackers are also leveraging workplace collaboration tools such as Slack, Discord and Microsoft Teams that exploded in popularity when the pandemic sent office workers home. Since collaboration platforms are a trusted part of an IT network, successful hacks thereof can bypass perimeter security protections to deliver malware or exploit legitimate application programing interfaces (APIs) to establish command-and-control protocols used to export data from target networks. Since users are accustomed to chatting with other workers across the enterprise, they are less likely to be hypervigilant when responding to a request from a "colleague." [12]

[10] Source: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[11] Source: https://healthitsecurity.com/news/fbi-spike-in-vishing-attacks-seeking-escalated-access-credential-theft
[12] Source: https://www.databreachtoday.com/search.php?keywords=Fraudsters+Flooding+Collaboration+Tools+With+Malware

Organizations should create enhanced security and awareness training for the organization's employees as well as the third-party vendors' employees who have access to sensitive data and stress the importance of the patient data they are handling.

Organizations should also be on the lookout for fake social media pages, as Johns Hopkins found out recently. A Facebook page purportedly from the health system was created in November 2020, with four of the 10 initial posts aimed at employee recruitment. Despite the recent page creation and questionable spelling, including misspelling the health system's name, several people responded to the page, which was traced to a cryptocurrency exchange website in Nigeria. [13]

Organizations are continuing to spend significant resources to reduce security risk, but some breaches are caused by simple human mistakes. Although the reason for many of the breaches reported to OCR over the years has been the result of a ransomware attack, other reasons include inadvertently mailing or emailing PHI/ePHI to the wrong recipients or sending ePHI through unsecured email. Organizations should create enhanced security and awareness training for the organization's employees as well as the third-party vendors' employees who have access to sensitive data and stress the importance of the patient data they are handling.

## Third Party Risk

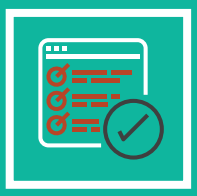
Although technology upgrades, proactive maintenance and constant monitoring of IT infrastructure can help keep healthcare providers safe from cyberattacks, employee security and awareness training is just as crucial to continually reinforce company policies and make the organizations aware of the threat landscape. This type of training and awareness must extend past your own organization and into the third party organizations leveraged by the healthcare providers.

Forty-three percent of breaches in the first half of 2021 reported that a Business Associate was present, as compared to 33% in the first half of 2020. As we saw in the Blackbaud and SolarWinds breaches, malicious actors were able to move laterally into other organizations undetected. No matter how well educated your employee base is on security and the associated threats, it is all for naught if you leverage a third party organization who does not adhere to security fundamentals which includes an effective security and awareness training program for its users.

[13] Source: https://www.beckershospitalreview.com/workforce/fake-johns-hopkins-medicine-facebook-account-spreads-false-job-listings.html?utm_medium=email&utm_content=newsletter

# Ways to employ the use of people, process and technology to combat these threats

Security and Awareness Training



Third Party Risk Management

Dark Web Monitoring

Multi-Factor Authentication (MFA)

Endpoint Detection and Response

**Pause to Consider**

1. What training do you offer workers on cybersecurity issues, and do you offer individualized training based on employee roles?
2. How often are employees required to enroll in training and how often is it updated to include new threat vectors?
3. Do your security policies apply and include requirements for your third party vendors?

# Responding to an Incident

When an incident occurs, an organization's goal should be to contain the threat, mitigate losses and return to an operational state as quickly as possible. Organizations who are prepared have certain exercises to run through and options to consider. Although it is advised not to pay a ransom to recover data or unlock systems, when an incident occurs it remains an option for organizations to consider. The average initial ransom demanded in the healthcare industry by threat actors in 2020 was $4,583,090, with the average ransom paid by healthcare companies being $910,335.[14]

## Federal Government Intervention

The federal government's has been making moves to curtail the payment of ransoms. In October 2020, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) released an advisory stating "companies that facilitate ransomware payments to hackers on behalf of ransomware victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, are violating OFAC regulations." [15] Although the payments are deemed illegal by OFAC, U.S. companies continued to be hacked and paid ransoms in the first six months of 2021.

In response to the recent surge of ransomware attacks that have crippled US infrastructures and disrupted businesses, the US Department of Justice (DOJ) stated it now prioritizes ransomware attacks the same way it handles terrorism cases, allowing the DOJ to work with the FBI to centrally coordinate information about ransomware attacks. "It's a specialized process to ensure we track all ransomware cases regardless of where it may be referred in this country, so you can make the connections between actors and work your way up to disrupt the whole chain," said John Carlin, principal associate deputy attorney general at the Justice Department.[16] In June, the Justice Department announced it successfully recovered approximately $2.3 million in Bitcoin that was paid to the criminal hacking group for the Colonial Pipeline ransom.

In May 2021, President Joe Biden issued an executive order strengthening cybersecurity regulations, saying that "the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security." [17] His infrastructure bill, which faces an uncertain future in Congress, also contains significant monies for information security.

## Cyber Insurance is Changing

In many situations, ransomware payments were covered by cyber insurance policies. Hackers are aware of this arrangement and use it as leverage against organizations in their ransom demands. Their thought process is if cyber insurance will cover the payment, there is no reason not to pay. However, this has caused the insurance industry to reevaluate how much coverage to provide and at what cost.

[14] Source: https://www.bakerlaw.com/press/bakerhostetler-2021-data-security-incident-response-report-security-disruption-and-transformation
[15] Source: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[16] Source: https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/
[17] Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Insurance companies are raising premiums for plans that cover damage from hacks. Prices for at least half of insurance buyers went up 10% to 30% in late 2020, according to a survey cited by the U.S. Government Accountability Office.[18] In June 2021, John Kerns, an executive managing director at insurance brokerage Beecher Carlson, a division of Brown & Brown told the *Washington Post* that "overall, ransomware claims have increased by upward of 300 percent in the past year." [19]

Insurance underwriters are taking a harder stance and demanding detailed proof of cybersecurity measures before approving coverage. Questionnaires about an organization's cybersecurity practices were used to write a cyber policy with few limitations. Now, attestations and proof of deployment are being used for increased security vetting by some cybersecurity insurance carriers, while others are declining to take new customers or capping amounts for existing customers.

Insurance underwriters are taking a harder stance and demanding detailed proof of cybersecurity measures before approving coverage.

## How Does the Healthcare Industry Proceed?

With the federal government's renewed focus and cyber insurers more stringent applications, it is clear there is a shift in liabilities. More liability is being put on healthcare organizations and they must be ready to bear the brunt of the blow.

"The best defense is a good offense" is often used to describe sports team tactics, but the phrase has its genesis in military conflicts, an apt comparison to today's cybersecurity environment where increasingly sophisticated attacks against hospitals and health systems occur almost daily. It is not enough to wait passively for an attack to occur. Cybersecurity professionals must be ever vigilant to protect against internal and external threats, and organizational leaders must prioritize information security resources and projects against many other competing priorities.

Early detection is a key component in any cybersecurity plan against these more sophisticated attacks. The healthcare industry has the dubious distinction of taking the longest average time to discover and contain a breach — 329 days. That is nearly 11 months; three months longer than the financial industry, which also handles extremely sensitive data and is governed by federal security regulations.[20] The healthcare industry simply must get better at protecting against unauthorized intrusions and the innocent or deliberate employee actions that threaten sensitive information.

Protecting health information is a tall order for many organizations. IT staff members are spread thin and usually generalists in technology matters, rather than the cybersecurity experts tasked to proactively protect a hospital's vital information and systems. Hospitals continuously compete for cybersecurity expertise, which is in great demand. In May, the U.S. Commerce Department estimated about 465,000 nationwide cybersecurity openings. [21]

Given these competing demands for time and money, we continue to see many hospitals and health systems choosing to outsource their cybersecurity monitoring and remediation efforts, leaving specialized tasks to experts well-versed in the unique challenges that healthcare IT represents.

---

[18] Source: https://www.gao.gov/products/gao-21-477
[19] Source: https://www.washingtonpost.com/technology/2021/06/17/ransomware-axa-insurance-attacks/?utm_source=rss&utm_medium=referral&utm_campaign=wp_business
[20] Source: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf
[21] Source: https://www.msn.com/en-us/money/markets/thousands-of-jobs-in-cybersecurity-are-open-for-the-taking/ar-BB1gV1Cr

## Cybersecurity Is an Every Day Priority

Cybersecurity is more a journey than a destination. Threats are a constant, and your security program, which includes monitoring and remediation efforts, should never be one-and-done. Consider these seven steps to strengthen the information security at your organization:

1

**Know what is in your environment.** Few hospitals fully understand the number of IT connections and their breadth across the healthcare landscape. EHRs, PACS laboratory systems, pharmacy systems and more are obvious systems that maintain potential external connections, but each system and each device that connects to any of these core systems must also be monitored and protected. The proliferation of internet-enabled medical devices has exponentially increased the number of connections to EHRs, and a security solution can automate the identification, assessment and protection of connected devices. Federal efforts to increase connectivity among providers are also bringing new challenges.

2

**Have an incident response plan.** The first step is to create proactive policies and plans to govern the IT network and employees. Creating an incident response plan is a critical step toward responding effectively to an attack, as proper preparation will facilitate a faster response when an incident is discovered. Leveraging a third party who performs these types of services to assist in the review or development of an incident response plan may allow your organization to achieve maturity quicker than performing it in-house. Plus, an independent perspective is also beneficial in identifying areas for improvement.

Creating an incident response plan is a critical step to responding effectively to an attack as proper preparation will facilitate a faster response when an incident is discovered.

3

**Get your employees on board.** How often does your organization conduct employee training on cybersecurity policies and procedures? People are often the weak link in the cybersecurity chain, falling victim to phishing, pharming or email account compromise attacks. Every employee who has access to IT systems and sensitive data should, at the bare minimum, receive training annually to reinforce policies and refresh memories about information security. Security reminders in employee communications can help. Some organizations also test the effectiveness of their employee security and aware training program by performing internal phishing campaigns and monitoring the response, retraining and educating those individuals who fail the test. This type of training is especially important to the executives, IT administrators, network teams and account and finance teams within the organization, as they are often specifically targeted.

4 **Conduct risk assessments and test your plan.** Understanding your organization's vulnerabilities and testing for the most likely scenarios will help staff respond more quickly and efficiently to an actual event. Think of it this way, if you need emergency surgery, do you want a surgeon who always operates on a set schedule or one who constantly deals with emergent cases? Likewise, putting a plan into action should be second nature to cybersecurity veterans who have planned for this eventuality.

5 **Restrict user access.** When possible, access to IT systems should be restricted to only those who explicitly require it. For example, medical and billing staff obviously need to interact with the EHR, but the HR department may not. Does every employee really need an email account, and if so, are they required to access it outside the organization? Restricting access, requiring multi-factor authentication or single sign-on, and providing regular education can help protect systems. By limiting user access to the minimal amount required, cybersecurity teams reduce the potential attack surface, which reduces risk.

6 **Do not rely on cyber insurance.** Cyber insurance rates rose as much as one-third in late 2020 because of the considerable increase in ransomware attacks. In addition to raising rates, insurers are hiking deductibles, limiting their exposure and demanding certifications as a prerequisite to offering coverage. The average ransomware payout quadrupled during 2020, significantly increasing the exposure of insurance companies. You can still get cyber insurance but be prepared to pay dearly for it. Cyber insurance is a transfer of risk above the threshold that has been identified by your organization; it is not a security control. The organization must be proactive in maintaining its security program and the associated controls to minimize the likelihood of an incident.

7 **Think about outsourcing.** Cybersecurity functions are critical to the practice of healthcare but may not be resourced appropriately or with well trained, qualified cybersecurity professionals. While IT staff may be needed to maintain computers and servers, most IT functions can be outsourced to a third party with specialized skills and guaranteed service levels. In particular, cybersecurity is best left in the hands of those with specialized skills and particular healthcare knowledge and expertise.

Until the healthcare industry starts to show resilience in the face of unrelenting malware and ransomware attacks, they will continue. Hospitals and health systems need basic mechanisms for both security technology and security processes to protect themselves and their patient data. Protecting critical infrastructure and data is not for the faint-hearted, as attacks become bolder and connections among healthcare technologies grow in number and sophistication.

**Pause to Consider**

1. Does your organization have an incident response plan? If so, when was the last time it was updated?
2. Do you have an incident response retainer in place to help make sure your organization is appropriately supported during a time of need?
3. How strong is your IT staff on cybersecurity issues? Would outsourcing your cybersecurity program benefit your organization?

Fortified HEALTH SECURITY

# Contact us to learn more about Healthcare's Cybersecurity Partner®

**For more information, visit our website at:**
fortifiedhealthsecurity.com

**Inquires**
1 (615) 600-4002

**Office**
2550 Meridian Blvd, Suite 190
Franklin, TN 37067

## About Fortified Health Security

Fortified Health Security is healthcare's recognized leader in cybersecurity – protecting patient data and reducing risk throughout the Fortified healthcare ecosystem. As a managed security service provider, Fortified works alongside healthcare organizations to build tailored 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. Fortified's high-touch engagements and customized recommendations maximize the value of investments and result in actionable information to reduce the risk of cyber events. The company is 100% committed to creating a stronger healthcare landscape that benefits more clients, protects more patient data, and reduces more risk.

## About the Authors

**Dan L. Dodson** serves as CEO of Fortified Health Security, a recognized leader in cybersecurity that is 100% focused on serving the healthcare market. Through Dan's leadership, Fortified partners with healthcare organizations to effectively develop the best path forward for their security program based on their unique needs and challenges. Previously, Dan served as Executive Vice President for Santa Rosa Consulting, a healthcare-focused IT consulting firm, where he led various business units including sales for the organization. He also served as Global Healthcare Strategy Lead for Dell Services (formally Perot Systems), where he was responsible for strategy, business planning and M&A initiatives for the company's healthcare services business unit. Dan also held positions within other healthcare and insurance organizations including Covenant Health System, The Parker Group and Hooper Holmes. Dan is a thought leader in healthcare cybersecurity and is a featured media source on a variety of topics. In 2018, Dan was recognized as a rising healthcare leader under 40 by Becker's Hospital Review and regularly speaks at industry-leading events and conferences including CHIME, HIMSS and HIT Summits. He served on the Southern Methodist University Cyber Security Advisory Board and currently serves on the CHIME Diversity and Inclusion Committee. Dan earned an M.B.A. in Health Organization Management and a B.S. in Accounting and Finance from Texas Tech University.

**William Crank** serves as Chief Operating Officer for Fortified Health Security where his responsibilities include enhancing the company's services, delivery model, and security operations center. As a member of the executive committee, William works to streamline operations among the sales, solution architect, account management, and customer success teams in addition to continually enhancing Fortified's expertise by attracting, training, and retaining top security talent. Prior to his role as COO, William was the chief information security officer (CISO) at MEDHOST, a provider of market-leading enterprise, departmental, and healthcare engagement solutions. He has decades of information technology and security experience that include managing the Information Security Risk Management (ISRM) team at Hospital Corporation of America (HCA), where he led a team of Information Security professionals who managed compliance and information security risk and developed and implemented an operational risk management model. William retired after serving 20+ years from the United States Navy. He currently holds multiple certifications in the areas of Information Security and Information Technology. William has also served as Sponsorship/Programs Director and Vice President of the Middle Tennessee chapter of the Information Systems Security Association (ISSA).


# Healthcare's Cybersecurity Partner®

fortifiedhealthsecurity.com