Fortified HEALTH SECURITY

2022 Mid-Year Horizon Report

The State of Cybersecurity in Healthcare

CEO's Message

Over the past several years of annual and mid-year Horizon Reports, the healthcare industry has made much progress toward adopting a security-first mindset and protecting health information and technology assets. That's the good news.

The not-so-good news is that the threats facing healthcare continue to evolve, grow at a faster rate, and become more sophisticated. More than 40 million patient records were reported as compromised just last year and reported healthcare data breaches remain the costliest among all other industries, with an average recovery cost exceeding $9.23 million. There's still a lot of work to be done to achieve a resilient and secure healthcare ecosystem which can successfully identify and defend against cyberattacks and attempted breaches.[1]

Topics for the 2022 Mid-Year Horizon Report vary widely, encompassing incident response, penetration testing, cyber program effectiveness, MITRE ATT&CK framework, and the growing dependence on artificial intelligence to propel cybersecurity efforts.

Underpinning each topic is the severe human capital shortage that industries — not just healthcare — continue to face. An international survey of cybersecurity employment shows a 400,000-job narrowing of the talent gap, from 3.12 million in 2020 to 2.72 million last year. However, the survey suggests that the global cybersecurity workforce must grow by 65% to keep pace with industry needs.[2]

Anecdotally, we don't see a lot of new talent at the CIO/CISO levels among the hospitals and health systems that Fortified partners with. New ways of thinking and new approaches may be required to overcome the cyber talent gap. Technology advances and the pandemic have made remote working easier than ever and greatly expanded the talent pool; however, facilities that insist on IT workers reporting to an office have a disadvantage in hiring and retaining staff. New thinking must also extend to human resource departments and the Board of Directors to tackle the talent shortage.

Jefferson Health, which serves greater Philadelphia and southern New Jersey, has made strides in this area by investing in entry-level workers, leveraging automated technology, and reducing burnout among current staff.[3] That may prove to be a successful model for other hospitals and health systems, as could outsourcing security monitoring to a trusted third party with deep expertise in healthcare cybersecurity.

The industry is also facing challenges obtaining cyber insurance, which often is a requirement for grants and other funding. Assessments from insurers are getting more robust with requirements for specific controls and technologies such as multi-factor authentication, third party risk management, and endpoint detection and response systems to mitigate the risks associated with the current threat landscape.

Finally, the U.S. Department of Health and Human Services is developing consensus-based best practices and methodologies for healthcare entities to improve their cybersecurity postures through the 405(d) Program. The task force has created Health Industry Cybersecurity Practice (HICP), pronounced "hiccup." The goal is to help the industry develop meaningful cybersecurity objectives and outcomes through proven cybersecurity practices and consistency in monitoring and mitigating cyber threats.[4]

I remain optimistic that hospitals and health systems will meet these cybersecurity issues head-on, and I trust that the Mid-Year Horizon Report will be a valuable resource for your cybersecurity program. We welcome your feedback and perspective at: horizonreport@fortifiedhealthsecurity.com. Enjoy!

Regards,

Dan L. Dodson

1 Source: https://healthitsecurity.com/features/exploring-challenges-benefits-of-cyber-insurance-in-healthcare
2 Source: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
3 Source: https://healthitsecurity.com/features/how-jefferson-health-is-tackling-the-cybersecurity-workforce-shortage
4 Source: https://405d.hhs.gov/protect

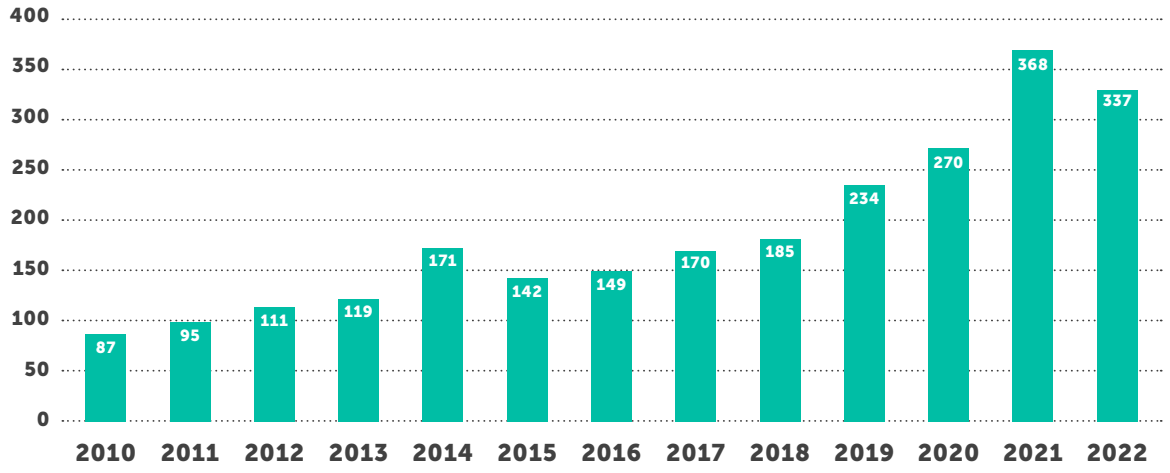
2022 Mid-Year in Review

While the number of healthcare cybersecurity reported breaches has leveled off after meteoric rises over the past several years, hospitals and health systems still cannot breathe a sigh of relief. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80% of all reported incidents.

A new survey of Chief Information Security Officers across industries showed that more than half (54%) believe the C-suite is not investing enough in cybersecurity. Nearly 90% reported having an incident response plan, but having a plan doesn't mean an organization is doing the day-to-day activities necessary to repel an attack. Remarkably, among those surveyed, 12% report discussing cybersecurity only after a breach had occurred.[5]

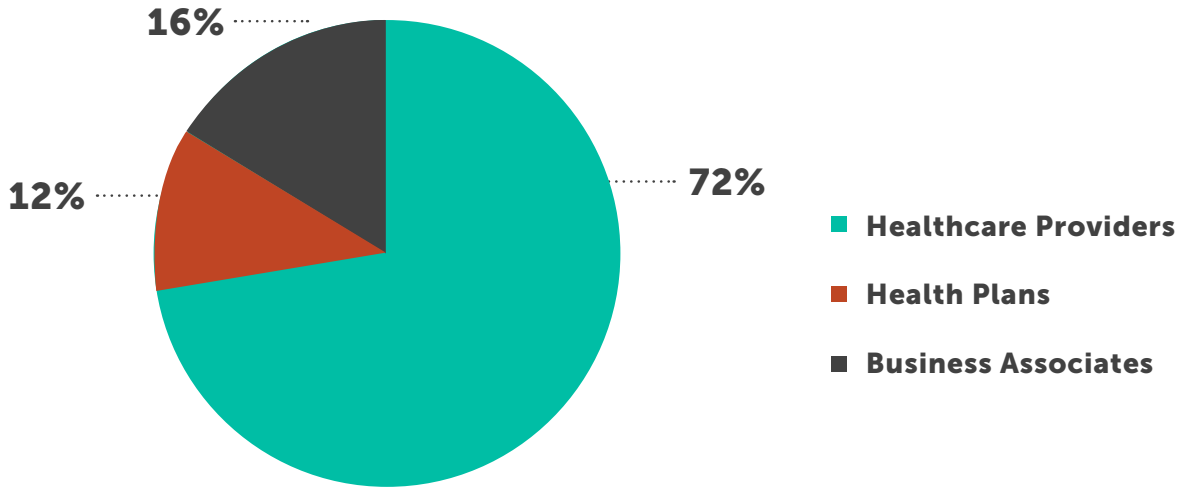
During the first half of 2022, the number of data breaches impacting 500 or more records reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR)[6] numbered 337. While that number is lower than the previous year at this time, it's on par with 2020 numbers through the first half of the year. Healthcare providers again account for the most breaches (72%), followed by business associates (16%), and health plans (12%). Interestingly, business associate breaches rose compared to last year, while health plan breaches decreased by a similar percentage.

Number of Breaches - First Half of Each Year



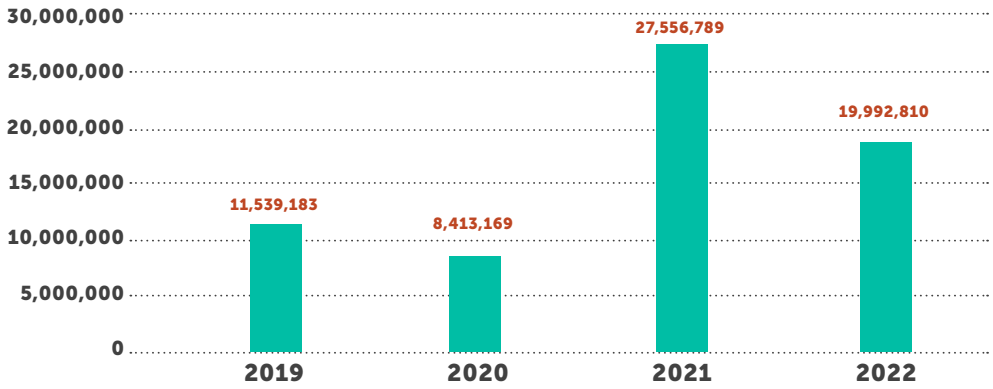
5 Source: https://healthitsecurity.com/news/54-of-cisos-struggle-to-convince-board-to-prioritize-cybersecurity-investments
6 Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Type of Entity Reporting the Breach First Half of 2022



In terms of number of records affected, 2022 numbers are down from 2021 by about 40%. 2021 was a record-setting year in terms of breaches, with 714 breaches impacting nearly 50 million patient records. But comparing breaches against the first half of 2020, the number of affected records is 138% higher, with more than 19 million records impacted so far this year. In terms of affected records, 2015 was the most infamous year, with more than 112 million affected records — 80% caused by Anthem and Premera Blue Cross breaches of nearly 90 million records. We hope not to see another year like 2015. One can certainly assert that after 2015, many organizations stepped up their defenses. But the attacks continue to evolve so those measures will not be enough moving forward.

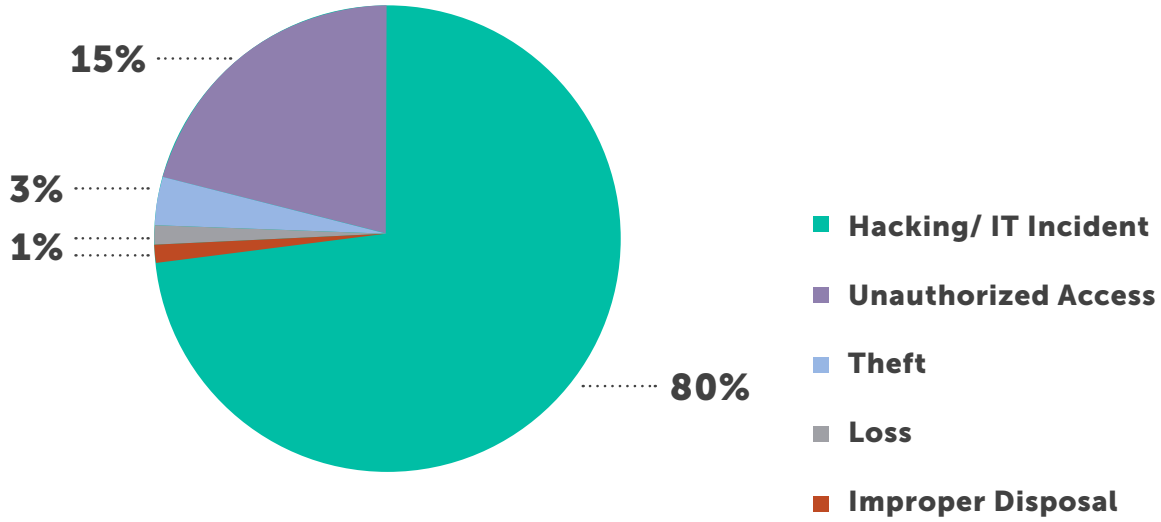
Individuals Affected First Half of Each Year



Equally disturbing is the small number of healthcare entities responsible for a large percentage of breached records. Seven entities experienced breaches of more than 490,000 records each, which account for 6.2 million records — 31% of the 2022 totals so far. Affected entities included a Florida hospital (1.35 million records), an imaging provider (2 million records), a California health plan (854,000 records), a business services provider (500,000 records), and a billing company (510,000 records). Attackers know where they can achieve the most bang for their nefarious buck.

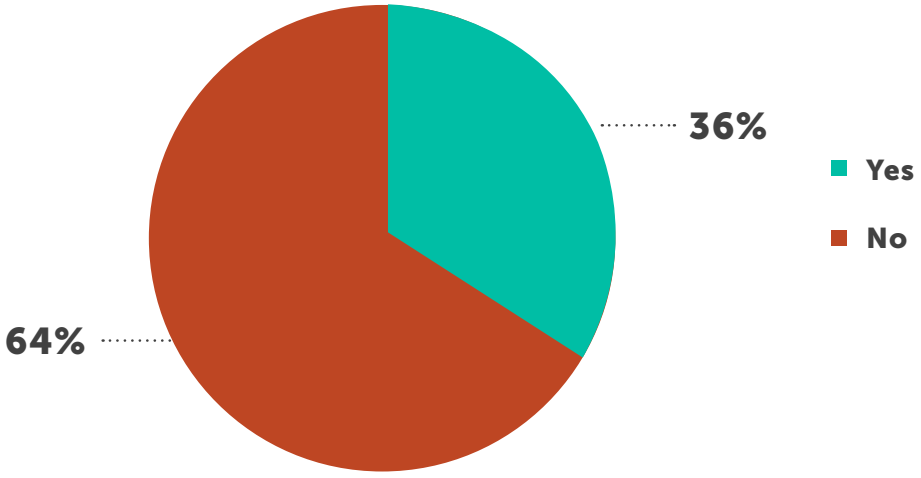
Malicious attacks ranked as the No. 1 cause of breaches for a sixth consecutive year, with the percentage of incidents pegged to hacking/IT incidents rising from 73% last year to 80% so far in 2022. Unauthorized access/disclosure accounted for 15% of incidents, with 5% attributed to loss, theft, and improper disposal of records or technology.

Type of Breach First Half of 2022



While the trendline from mid-year 2021 to today is down, overall breach numbers and affected records remain stubbornly high. The potential attack surface for hospitals and health systems continues to grow as employees work remotely and more medical, financial, and operational technologies move to the cloud.

Breaches Where Business Associate Was Present First Half of 2022



IT professionals face many challenges, including competition for limited corporate resources, a tight workforce, growing amounts of IT security data that must be monitored and protected, a workforce often working remotely, increasingly cunning bad threat actors, and humans susceptible to phishing and other types of attacks. The continued prevalence of healthcare cyberattacks should serve as a wakeup call for all healthcare leaders to assess their current security postures and take action to decrease risk and increase visibility and capability.

Pause to Consider

1. How resilient is your organization's cybersecurity posture to defend attacks?
2. What has changed in your healthcare environment over the past year, and how has your cybersecurity program adapted to those changes?
3. How are staffing issues affecting your ability to monitor, detect, and protect your critical assets?
4. Where does cybersecurity program and spending to fund it rank among C-suite priorities?

Do a Little Harm: Tactics to Gauge the Security of IT Environments

Fortunately, the Hippocratic Oath "do no harm" doesn't apply to healthcare cybersecurity professionals, who sometimes are tasked with trying to exploit security loopholes or weaknesses in healthcare infrastructure to validate risk and exposure to a cybersecurity incident.

The cybersecurity exercise, known as red teaming, uses the same tactics that bad actors deploy during their attempts to infiltrate healthcare IT systems. Tactics could include targeted spear phishing, social engineering, or the exploitation of any vulnerability the red team discovers during their simulated cybersecurity attack. Like an MRI or a blood test, the red team cybersecurity exercise is diagnostic in nature, designed to test the resilience of your healthcare cybersecurity program.

The execution of a red teaming exercise is the sign of a mature healthcare organization that has moved beyond foundational cybersecurity and should be an integral part of every hospital's security plan moving forward. Getting to that point requires many intermediate steps designed to create a security posture that is ready to be tested by a red team exercise.

"The execution of a red teaming exercise is the sign of a mature healthcare organization that has moved beyond foundational cybersecurity."

At each step along the way, IT leaders should keep C-suite stakeholders informed about the outcomes of vulnerability scans, penetration tests and any identified vulnerabilities and resulting cyber risk. Doing so underlines the importance of cybersecurity to keep patient data safe and the hospital or health system operating without interruption.

The first step in strengthening a comprehensive security posture is gaining visibility and understanding of the environment. Knowing what systems are in the network and which are most critical are vital to making informed decisions. A close second is a vulnerability management program, which provides an up-to-date picture of the security of an environment at that point in time. Vulnerability scanning, performed either in house or by a third-party vendor, should be accomplished frequently to keep up with changing hardware, software, and ever-evolving vulnerabilities. The National Vulnerability Database recorded over 19,000 vulnerabilities in 2020 and more than 20,000 in 2021. Any vulnerabilities discovered should be prioritized based on severity and exploit potential, then remediated to the degree possible.[7]

Penetration testing, often called "pen testing," uses the same techniques that attackers employ to find and safely exploit vulnerabilities to gauge the severity of IT system weaknesses and the potential for bad actors to move among systems or elevate privileges. Although the terms vulnerability scanning and pen testing are often used interchangeably, pen testing builds upon vulnerability scans by focusing on exploiting weaknesses rather than finding and categorizing potential risks.

7 Source: https://nvd.nist.gov/

Vulnerability scans are performed much more frequently; industry best practice is monthly, while a pen test is usually once or twice annually.

According to research firm ESG, nearly half (47%) of organizations believe that pen testing and red teaming are a best practice for risk identification and reduction.[8] While pen testing is not mandated for HIPAA compliance, standard 164.308(a)(8) requires periodic assessments of IT networks and systems, which can be accomplished through penetration testing or a simulated red team exercise.[9]

If red teams are the bad actors, then blue teams are the good actors trying to protect their IT environments. When they work together to evaluate the security of IT infrastructure, that's when a purple team emerges as a collaborative team – red and blue combined.

For example, if the blue team knows that a red team attack is imminent, the blue team may be more on guard to protect the infrastructure. At the same time, if a red team is composed of hospital or health system IT professionals, the red team understands the blue team tools and defenses. When you combine the teams forming a purple team, this is more of an execution of testing against the security construct itself to help ensure the environment is resilient and that defensive tools are tuned properly. During and post exercise, the teams can discuss whether the blue team recognized the red team's attack and the speed and strategy of the blue team in leveraging its tools to monitor, identify and defend against the attack.

The composition of the blue team and red team can also be influenced by organizational IT maturity, staffing levels, and the experience of that staff. According to the 2021 Cybersecurity Workforce Survey, 60% of study participants said the cybersecurity workforce gap is putting their organizations at risk.[10] Keeping staffing issues in mind, it's common for smaller security teams to handle basic, routine tests while using third party services for more complex tests. Few hospitals or health systems have dedicated blue teams (much less adversarial red teams), so outsourced testing services would make sense in those cases. Internal red teams may also be reluctant to exploit vulnerabilities in IT systems maintained by colleagues, another reason to consider hiring a trusted red team provider.

"Internal red teams may also be reluctant to exploit vulnerabilities in IT systems maintained by colleagues."

As an organization's IT infrastructure becomes more resilient through frequent vulnerability scanning and mitigating identified vulnerabilities and less-frequent penetration testing and red teaming, the stakes should increase with more targeted attacks from more experienced red teamers. During the first couple of years, the focus is likely on remediating the low-hanging fruit and patching the glaring vulnerabilities and performing required fixes.

8 Source: https://www-csoonline-com.cdn.ampproject.org/c/s/www.csoonline.com/article/3652597/operationalizing-a-think-like-the-enemy-strategy.amp.html
9 Source: https://fortifiedhealthsecurity.com/blog/6-considerations-for-hipaa-compliant-penetration-testing/
10 Source: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

As the organization becomes more security conscious and utilizes more capable detection tools, the intensity of attacks should ramp up in response to the increasing maturity of the organization.

Success for a security operations team means reducing the attack surface through proactive processes such as vulnerability scanning, pen testing, and red teaming, deploying cybersecurity tools, and developing the ability to detect and respond to threats before serious impacts can occur.

Adopting a proactive security approach with a comprehensive monitoring and detection capability will serve as the first line of defense, placing significant obstacles in the path of potential bad actors so they look for easier prey, effectively raising the cybersecurity fence protecting your healthcare organization and keeping patient healthcare secure and available.

"Adopting a proactive security approach with a comprehensive monitoring and detection capability will serve as the first line of defense."

It is important, especially in an organization's early adoption of these practices, to not view red team success as a criticism of any specific person or system. It merely identifies a current vulnerability and allows for the establishment of baselines from which the organization can grow and become stronger. From there, these internal attacks should become a key component of your ongoing cybersecurity efforts.

Pause to Consider

1. How often does your organization perform vulnerability scans and penetration testing?
2. What process is in place for IT staff to remediate system weaknesses and vulnerabilities identified, and what is the timeline?
3. Is your IT department equipped to perform red team exercises in-house, or should you consider engaging a trusted provider?
4. How do you communicate IT security issues to the C-suite? Do you maintain a centralized risk registry or provide frequent risk reporting?

Emerging AI/ML IT Security Offerings Can Strengthen Cyber Infrastructure

In the hospital emergency department, the speed of care delivery can be life-altering/saving for patients. Physicians and staff must make split-second decisions that affect the course of treatment: making diagnoses, administering life-saving medications, or referring patients for immediate surgery.

Artificial intelligence (AI), machine learning (ML), and deep-learning technologies are transforming diagnoses and healthcare delivery, performing some of the heavy lifting to give human caregivers time to make more deliberate decisions while working at the top of their licenses.

Likewise, advanced technologies that leverage AI/ML concepts are also transforming IT security services that can bring quicker threat detection and mitigation, increased productivity, and the ability to perform sophisticated tasks with fewer staff or extend the capabilities of junior security staff members.

For example, consider security information and event management (SIEM) software, which monitors IT infrastructure for potential security threats. SIEM platforms consume log data from IT monitoring systems such as end point protection software, firewall, email security systems, and intrusion detection tools, normalizing the data, prioritizing the threats, and presenting the data in near real time for analysis in an easy-to-read format like a dashboard. Depending on the vendor and how the platform is configured, the technology can morph in response to new or emerging threats to perform the labor-intensive tasks associated with log analysis that formerly fell to IT staff.

AI/ML detection and response technologies promise many advantages to healthcare organizations that likely face stiff competition for workers. Continued remote work and the trend to move IT services to the cloud extend a hospital's four walls and put additional pressure on your cybersecurity program and staff. The day-to-day pressures can take IT staff away from "eyes on glass" monitoring activities. Leveraging AI/ML security technology can free up higher-level IT staff to concentrate on bigger-picture security issues and emerging threats.

"AI/ML detection and response technologies promise many advantages to healthcare organizations that likely face stiff competition for workers."

Emerging technologies allow greater visibility into the IT environment, comparing network behavior against expected behaviors; for example, a login attempt from an unexpected location or someone with clinical system access trying to access financial systems.

Healthcare IT staff are well aware that the industry has the highest costs associated with a data breach, estimated at $9.23 million per incident — the highest cost of any industry for 11 consecutive years. However, the latest report shows that organizations that leverage AI and automation can detect and contain breaches 27% quicker than those without.[11]

Organizations with no security AI/automation took an average of 239 days to identify a breach and another 85 days to contain it. In comparison, organizations with fully deployed security AI/automation needed 184 days to identify the breach and 63 days to contain it — the difference between nearly 11 months to find and contain a breach versus 8.2 months with AI technology.

Time and personnel savings from deploying and operationalizing AI/ML solutions can be used to raise an organization's overall IT security awareness. More than eight out of every 10 healthcare data breaches involved an unwary human through the use of stolen credentials, targeted phishing, misuse, or errors, so continual employee training and security awareness throughout the organization must be a focus.[12]

The emerging importance of AI/ML security technologies doesn't mean hospitals must rip-and-replace software and completely redesign workflows. Any investment involves tradeoffs among what a tool is expected to do, its cost, and the time/effort required to deploy that tool effectively throughout the organization. Depending on an organization's size and IT maturity level, some technologies — however effective — may not be worth that time/money/effort.

Making those choices may be difficult, which is where a third party IT consultant or managed security services provider can help. A partner can provide an agnostic assessment of an organization's security program, evaluate the technology currently in use, and offer suggestions for different or complementary technologies to plug security gaps or provide additional layers of defense.

"Be wary of consultants who don't consider an organization's current technology, staff, and cyber maturity before making suggestions."

Be wary of consultants who don't consider an organization's current technology, staff, and cyber maturity before making suggestions. Such an approach is likely to be costly and may not deliver the results your organization is seeking. You want a partner who understands your complete picture and has deep experience in the healthcare sector.

11 Source: https://www.ibm.com/downloads/cas/OJDVQGRY
12 Source: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

Every industry is facing a do-more-with-less mentality, fueled by staffing issues, an ailing global supply chain, and the continual need to increase productivity. The stakes are among the highest in healthcare, a combination of providing patient care services 24/7/365, a wide-ranging IT network infrastructure, and the value of healthcare information.

Think about healthcare cybersecurity this way: the bad actor only has to be right once to gain the keys to the kingdom and unlock valuable healthcare information; the security team protecting that environment has to be right all the time. An overlapping cybersecurity strategy that includes AI/ML technologies can help hospitals and health systems gain the visibility they need into IT environments, improve their security postures, and extend the reach of IT staff.

Pause to Consider

1. How are labor shortages impacting IT staff and their ability to protect your infrastructure?
2. What technologies does your organization need to strengthen its security visibility and overall security posture?
3. How could your organization benefit from AI/ML IT security technologies?

Metrics: Tracking Data That Affects Patient Outcomes

Earlier, we spoke about a lack of focus around cybersecurity budgets, but we think that is only part of the story. Most often, budgets are applied to new projects with very little consideration for increased spend maturing existing controls. We understand that projects help move the business forward but, many times the operations side of cybersecurity is what matters most. Maximizing cyber spend means squeezing every ounce of value out of existing controls. Having a plan for maturing tools/controls once the official project is closed and the professional service hours are all used up helps ensure the ongoing resiliency of any cybersecurity program. Tracking and reporting operational metrics around cybersecurity are critical to proper cyber hygiene.

With so many possible avenues of attack, it's hard to know which cybersecurity metrics to prioritize. How many viruses/attacks were observed this month? Are we tracking the root cause of attacks? By what percentage has user awareness increased this year? How many patches were successfully deployed this month versus how many should have been deployed? What is our mean time to acknowledge an attack? What about our mean time to complete an investigation and remediation of those attacks?

> "Measure the factors that could affect availability, because availability affects patient outcomes."

The answer is actually simpler in healthcare than in other industries — measure the factors that could affect availability, because availability affects patient outcomes. If you were locked out of your EHR right now, how long would it be before you had to turn away patients?[13] Cybersecurity is such a large and complex topic, it is easy for a particular metric or threat to grab your attention, but maintaining the ability to treat patients must always be priority one.

There are two corollaries to this focus. First, make sure not to get so far into measuring tool effectiveness or the cybersecurity team's efficiency that you forget about the human factor. Verizon's latest global data breach investigations report found that a whopping 82% of breaches and cyber incidents involved a human element such as stolen credentials, phishing, misuse, or an error. Make sure to include human-related data points such as user-awareness training effectiveness and email click-through rates.[14]

Second, figure out a way to equate IT hours handling various cyber events so you can accurately calculate ROI on monies spent, whether on tools or outsourcing.

13 Source: https://healthitsecurity.com/news/ky-hospital-systems-down-during-cybersecurity-incident-investigation
14 Source: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

A basic, but important, use for metrics is finding coverage gaps. For example, your firewall is configured to block connections to hostile nation-states. What happens when an executive takes their laptop home and accesses the internet without that protection? Documenting your security controls and measuring how many of your systems are protected by those controls are key to starting mitigation should a problem arise.

The same is true for asset compliance: have you implemented an asset management solution; do you have an updated asset inventory; and are you alerted when an asset is missing a security control like a security vulnerability patch? Have you documented the clinical and vendor managed systems on your network that cannot be protected by some of your controls?

A similar use is measuring ROI. When you purchase a tool, you know how much you spent on it, and you can measure your organization's baseline before implementing it. For example, the organization's user click-through rate was averaging 30%; you spent $X on a user-awareness platform, and it resulted in a 3% average click-through rate. That was money well spent, and similar calculations are possible when outsourcing a portion of your cybersecurity tasks.

As mentioned above, determining how many hours an event takes can lead to useful statistics. Your cybersecurity team stopped 15 viruses this month, and your data shows each virus takes five people 10 hours to handle. Given that there are also soft costs involved (i.e., downtime and impact to patient care), these stats may help justify the purchase of more robust end point protection software.

It's also important to measure trends over time. For example, are the results of your penetration tests improving year over year? How many phishing attempts resulted in click-throughs from your users each quarter this year?

Beyond these basics, a key metric category is intrusion response and recovery. Are you running tabletop exercises to accurately measure how long it takes your team to identify and respond to mock incidents? How long will it take to identify the threat and remediate it before it can be exploited?

It's important to track those metrics accurately over time to gauge efficiency. Long dwell times (the time between the attacker's initial penetration and the point at which you know the attacker is there) are perhaps the most serious problem for hospitals. Although it's bad news, if attackers consistently linger in your systems (stealing your data and possibly planning a ransomware attack), you need to know. Armed with the facts, you can move forward by adding staff, tools, and/or outside help.

It's also a good idea to keep track of any backlogs. For example, software patches come in fast and furious these days, so prioritization is essential. But once you've applied the 300 most critical patches this month, is someone following up on the patches deemed less critical? Is your patch backlog becoming so overwhelming you will never get caught up?

A similar approach must be taken with threat remediation. If your team identifies 100 threats

in January but only remediates 50, and the same happens in February, you start March with a significant backlog. Keeping track of backlogged items is a "back-door" way to identify areas needing attention, ensuring you don't get to the point where only priority items are being worked on.

Finally, give careful thought to how your metrics are presented to various constituents. Obviously, your CIO is interested in a detailed account of your security posture. The CEO and Board of Directors likely prefer a high-level risk-based overview with minimal statistics, but that may not be true for significant security incidents, when they may want to hear details.[15]

Pause to Consider

1. What security metrics are you currently monitoring in your organization?
2. How does that differ from the security metrics you *should* be monitoring?
3. What programs are you using to train/monitor employees on cybersecurity issues?
4. How is your security posture changing over time?

15 Source: https://www.csoonline.com/article/3658118/cybersecurity-metrics-corporate-boards-want-to-see.html

Get Your Priorities Straight: MITRE ATT&CK Helps Cut Through the Clutter

One thing is certain: we cannot expand the number of hours in our day. For cybersecurity professionals, that translates to a near-constant need to determine which aspects of your organization's security are a priority. Fortunately, the open-source tool MITRE ATT&CK® makes it easier for cybersecurity professionals to learn about the most recent advanced persistent threats (APTs), while giving IT and business leaders a common lexicon to talk about them.

ATT&CK stands for Adversarial Tactics, Techniques and Common Knowledge and is a database of bad-actor tactics, originally developed for a MITRE research project to improve post-compromise detection of adversaries operating within enterprise networks. MITRE takes publicly available threat intelligence and incident reporting and distills it into a database of common tactics, techniques, and procedures (TTPs).[16]

For example, your firewall is configured to prevent a nation-state hacker from beginning a conversation with an asset in your organization. The firewall picks up on a possible intrusion, prevents it, and sends an alert to IT: a common occurrence. But imagine a computer inside your enterprise is trying to contact a bad actor in a nation-state. There's a strong possibility that computer is infected, warranting a fast response. IT can use the ATT&CK database to quickly research current tactics being used by specific nation-state hacker groups — are any of these showing up on the infected computer?

The information in ATT&CK is detailed and updated bi-annually. It notes which groups are using vulnerability scanning to actively scan networks, which are using phishing emails to gain a virtual private network (VPN) login they use to access admin credentials via PowerShell, and which are using the Start-Process command after gaining network access. This gives threat hunters a clear indication of where to begin their work.

Just as important, your cybersecurity team can leverage the information in ATT&CK to look for gaps in your defenses. Using ATT&CK Navigator, a cybersecurity professional can map the protections you have deployed back to the ATT&CK database. Results shown in green indicate a threat that can be detected and prevented. A yellow result is a threat into which your organization has visibility, and a red result is a threat into which it doesn't (a problematic gap requiring remediation).

> "Your cybersecurity team can leverage the information in ATT&CK to look for gaps in your defenses."

One of the major benefits of ATT&CK is its accessibility. It's designed to be understood by non-technical executives, providing a common ground for IT and business leaders to discuss potential security improvements, along with terminology that IT workers can use with their peers.

16 Source: https://attack.mitre.org/

Rather than having to describe exposed ports running services with a particular vulnerability that could lead to remote code execution (what executives consider geek speak), the ATT&CK framework uses layman's terms. For example, a cybersecurity expert might say a certain group exploits a vulnerability that allows them to maintain access to the network, move laterally from one system to another, and gain additional control of the network by elevating privileges.

The way cybersecurity is discussed is more important than ever. Most businesses are entirely dependent on technology (when was the last time you made a phone call on a landline?), so business leaders have a vested interest in making sure it works dependably. That necessitates a common language that levels the playing field — technology workers don't have to dumb down their explanations, and business folks don't have to learn cybersecurity acronyms.

Being proactive about preventing the type of cyberattack that shuts down your hospital's systems is no longer a nice-to-have. The cost of maintaining a strongly protected network pales in comparison with the cost of having to rebuild your organization's systems after a ransomware attack, not to mention the disruption to patient care.[17]

"Being proactive about preventing the type of cyberattack that shuts down your hospital's systems is no longer a nice-to-have."

Common frameworks, like ATT&CK, help cybersecurity teams and business leaders come together to discuss costs related to strong defense systems. Most of us have experienced the theft of a credit card number resulting in purchases being erroneously charged to us. Although disturbing, a phone call to your credit card company is all it takes to have the charges taken off the account.

Imagine that was not the case, that when you called the bank, the customer service person said you should have paid more attention to your account and that you were responsible for the entire bill. This scenario brings into sharp focus the importance of strong cyber defense, especially in light of the growing sophistication of hackers.[18]

Meaningful conversations about security priorities and the best way to reduce cybersecurity risks begin with understanding the true cost of a major attack, all the options for risk reduction, and all the tools available to help with prioritization.

Pause to Consider

1. Is your team using MITRE ATT&CK to understand gaps in your detection and response?
2. Do you understand your current exposure to cyberattacks based on the MITRE ATT&CK framework?
3. Have you asked your technology and services vendors whether they're considering threats contained in ATT&CK in their security plans?

17 Source: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/05/18/ransomware-attacks-on-hospitals-put-patients-at-risk
18 Source: https://cybersecurityventures.com/whos-more-sophisticated-hackers-or-your-security/

Incident Response: Mature Your Plan to Prepare for Major Intrusions

It is a moment every cybersecurity leader has thought of and dreads. You receive a phone call letting you know your patient information is being sold on the Dark Web, a splash screen on your monitor saying your systems have been infiltrated, or an emailed ransom note. No matter how the news reaches you, your stomach does a flip as you realize this is going to be one of the worst days of your life.

Let's start with the bad news. Hacker attacks on healthcare networks have not abated, and some types of attacks have increased in frequency. A technique known as living off the land in which threat actors use tools already in your environment to gain access (instead of bringing in malicious tools) means hackers are sometimes able to operate in your environment for weeks, months, or years without being detected.[19]

This allows them to execute a multi-staged attack. First, they quietly gain access. Second, they analyze your systems and data to determine what resources are available for use in other attacks or they identify and steal as much data as possible to sell on the Dark Web. Next, they penetrate further into your systems with the intent to lock you out or create disruption, and finally demand a ransom to further monetize their activities.[20]

The continued attacks on healthcare networks are also bad news in terms of hoping to escape a serious incident involving stolen data and/or a ransomware attack. Healthcare data is so valuable to hackers it's no longer a matter of if your hospital will be attacked but when it will happen. Some small- and mid-sized hospitals, especially those far from metropolitan areas, shrug off the danger. They mistakenly believe hackers target based on hospital size, location, or some sort of personal vendetta. This couldn't be further from the truth: there are databases of hospital operational data for sale to bad actors, and they simply check each hospital on the list looking for systems that aren't well-protected. Also, bad actors can assume that smaller, rural, hospitals — while hosting fewer records — will most likely have smaller defense teams, budgets, and systems. Criminals love the path of least resistance.

There's more bad news when it comes to protecting against threats via connected medical devices and service providers (e.g., the large breach of HR company UKG). These infiltrations tend to be particularly damaging because if a bad actor can appear to be a trusted partner, they can wreak severe havoc before anyone realizes the system has been compromised.[21]

19 Source: https://www.scmagazine.com/analysis/ransomware/ransomware-groups-keep-healthcare-in-sights-selling-access-on-the-dark-web
20 Source: https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html
21 Source: https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/ukg-hack-fallout-includes-lawsuits-data-breaches.aspx

Finally, there is bad news on the insurance front. The number of large, breach-related payouts in recent years is causing insurers to tighten their cybersecurity requirements. In the near future, hospitals will likely experience refusals to insure if their cybersecurity programs are found inadequate.

"The number of large, breach-related payouts in recent years is causing insurers to tighten their cybersecurity requirements."

Now for the good news. Although protecting against and recovering from cyberattacks isn't simple, it's by no means impossible. By focusing on the fundamentals, recognizing a few truths about attackers, not being afraid to conduct a true evaluation of your current security posture, and putting a strong incident response (IR) program in place, you can protect your company from the worst-case scenario.

The first step in preventing a major incident is ensuring the right people are assigned to the right roles, that those people have the right visibility and tools they need to be able to see potential issues, and that the right processes are in place to ensure essential steps are taken when there's an issue. This combination of people, process, and technology is key to making sure there are no gaps in your cybersecurity strategy.

For instance, it's not enough to have tools like network-based monitoring and intrusion detection; you must route the resulting logs to a secure location so they can be accessed in the event of a ransomware attack. System, application, network, data-access, user-access, and email logs are all key to determining how a bad actor penetrated the network, which areas they touched, and who they may be. They must be stored offsite, either in the cloud or at a managed service provider, so they're available for investigative purposes in the event of a network lockout.

The next step is helping everyone in your organization understand why the security measures IT implements are important. It's easy for IT to become complacent and believe that employees understand cybersecurity risks — they don't. Remember, while security is at the forefront of all our efforts, sadly for the hospital staff, it is often seen as just one more thing between them and the care they try to deliver.

- **To employees:** We don't have long passwords and multistep authentication just to drive you crazy; it's to prevent a bad actor from infiltrating our network and holding our network for ransom.
- **To executives:** We need cybersecurity professionals to constantly tune our firewalls and patch our system to prevent hackers from accessing our systems and stealing our data.[22]
- **To everyone:** Please attend our training sessions so we can prevent bad actors from gaining information via social engineering, email phishing, SMS phishing, and voice phishing. Cybersecurity is not just IT's responsibility; everyone is responsible for making sure our organization stays secure.

The final step is creating an IR plan. It's a good idea to have an expert evaluate your current capabilities and systems, suggest changes to close security gaps, and help you write a plan that can be followed by anyone at the company in the event of a system attack.

22 Source: https://healthitsecurity.com/news/log4j-vulnerabilities-put-strain-on-overburdened-cybersecurity-workforce

> "Cybercriminals deliberately schedule ransomware attacks to occur just before a weekend, often a holiday weekend."

Note that cybercriminals deliberately schedule ransomware attacks to occur just before a weekend, often a holiday weekend. They know senior managers are probably out of the office and may be unavailable by phone.

The plan must include contact information for notifications (executives' phone numbers, legal representatives, IT leaders, and any external IR service providers). It should outline the steps for IR responders to take first, including retrieving logs and confirming integrity of system backups stored offsite. Someone should begin investigating the extent of the breach and identify the source of the intrusion. If you have contracted with an outside firm to help with IR, that firm will often work on damage-control and determining the intrusion source while in-house IT focuses on getting the organization's IT assets back up and operational.

The time to contract with an outside firm is, of course, before an incident occurs. Trying to get a team on board after the fact is definitely more stressful and likely much more expensive. Additionally, part of the IR development process with an expert is conducting an incident response readiness assessment and could include an IR exercise in which a major breach is simulated and the company goes through its response plan as though it were the real thing. You may still feel your stomach drop if you receive notification of a system lockout, but at least you'll know exactly what to do.

Pause to Consider

1. Do you have an incident response program in place? If not, why not? And if so, when was the last time the incident response plan was updated?
2. Where are your security event logs stored and what timeframe do they cover?
3. Where are your backups stored and when were they last tested?
4. How often do you train employees on cybersecurity and what methods do you use to test the effectiveness?

Fortified HEALTH SECURITY

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

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

Inquiries
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 provide ROI 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 including security best practices, data privacy strategies, as well as risk management, mitigation and certification. He was elected to the Association for Executives in Healthcare Information Security (AEHIS) Board of Trustees in 2022. 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. 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).

Fortified
HEALTH SECURITY

Healthcare's Cybersecurity Partner®

fortifiedhealthsecurity.com