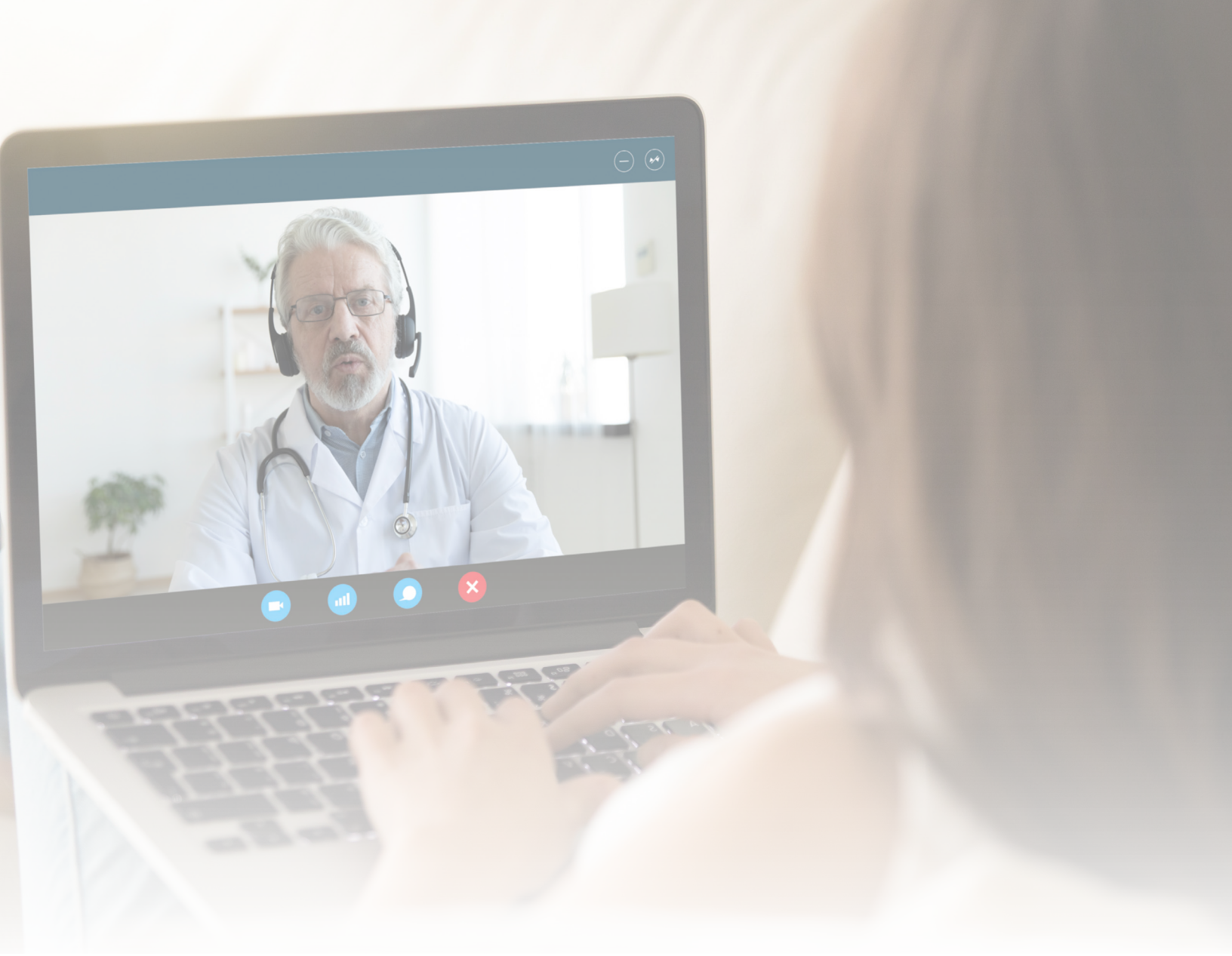


Fortified
HEALTH SECURITY

2021 Horizon Report

The State of Cybersecurity in Healthcare

CEO's Message

If cybersecurity wasn't on the radar of healthcare C-suite executives before the FBI's late October warning of an "imminent" threat to hospitals, it certainly is now. Couple that with ransomware continuously dominating headlines, highlighting how health systems have been brought to their knees as a result of outages impacting their ability to deliver care, and we may finally have the attention of our constituents. The seemingly ever-increasing amount of cybercrime directed toward the nation's hospitals serves as a wake-up call that the healthcare industry has desperately needed.

The healthcare sector has long been a target for hackers due to the sensitive nature of patient data flowing through healthcare IT systems and the lack of robust, mature security programs. Healthcare data is highly prized on the dark web since it can be used to create new identities, making it more valuable than credit card information. The threat of ransomware continues ,and given the COVID-19 pandemic, the potential impact to care delivery has never been higher.

COVID-19 has defined 2020 for hospitals and health systems that scrambled to meet an early spring surge in most areas and are dealing with still higher caseloads as this column is written. If there is a theme for this year's CEO Message, it's the idea of getting back to security fundamentals, taking a fresh look at your security infrastructure, your potential gaps and opportunities, your response plans, and your staffing model, to minimize cybersecurity risk and protect patients in the most cost-effective way. To increase preparedness, organizations are dusting off their incident response plans and devoting more time to updating and testing them. Cybersecurity leaders also are taking a closer look at the security tools they've purchased, with an eye toward eliminating redundant and perpetually licensed solutions.

COVID-19 has defined 2020 for hospitals and health systems.

The pandemic has also highlighted the need for adequate data security as many hospital employees started working remotely, greatly increasing the number of endpoints that needed protecting. Remote work arrangements and the meteoric rise in telehealth visits put new strains on the cybersecurity team in terms of security policies, continued employee awareness and training on email, and device security. The pandemic has brought into sharp focus the need for continual security monitoring and the growing realization that cybersecurity employees don't need to be physically in a building to be effective. This opens opportunities for hiring remote security staff, as well as outsourcing certain security functions so networks can be monitored and secured 24/7 using best-in-breed solutions by companies with specific healthcare experience.

We want the Horizon Report to underline the importance of cybersecurity in your organization and spark ideas that you can use to build awareness and improve your security program. We also value your feedback and perspective at: horizonreport@fortifiedhealthsecurity.com. We hope you enjoy the 2021 Horizon Report!

Regards,

Dan L. Dodson

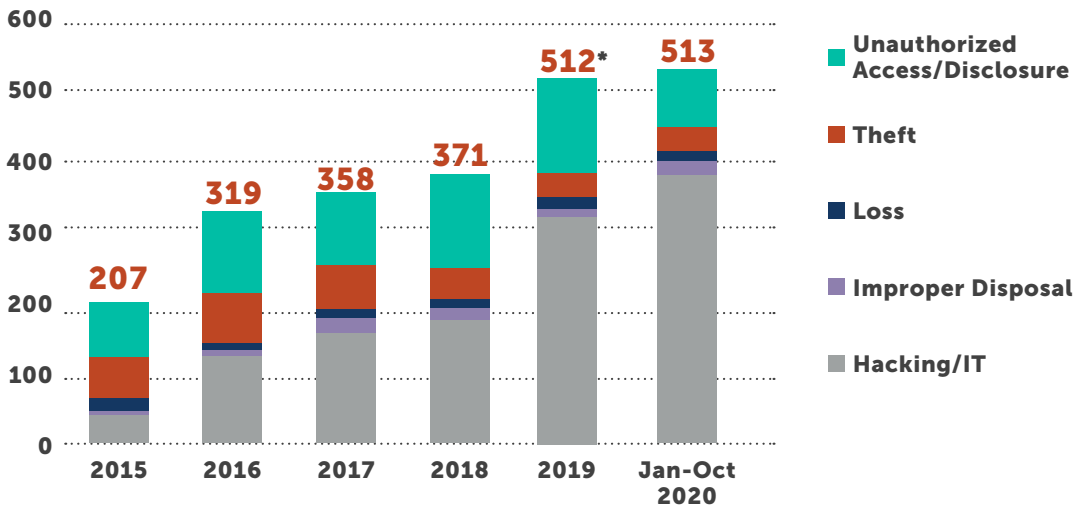
2020 Year in Review

As healthcare organizations continue to respond to the pandemic, cybercriminals persist in their attacks on providers, health plans, and business associates. More than 500 healthcare organizations have reported a breach of 500+ patient records to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) through the first 10 months of this year, and we expect that number to surpass 550 by the end of 2020. In total, 513 entities have reported a significant breach so far, equating to 23.5 million individuals impacted.[1]

Providers continue to be the most targeted sector, accounting for 79% of all reported breaches.

Through the first 10 months, the number of reported breaches increased 18% compared to the same period last year. This number is no surprise to those watching cybersecurity trends — cybercriminals began taking advantage of the chaos caused by the pandemic almost immediately and have not let up. In April, the FBI warned healthcare organizations and consumers that criminals were actively manipulating the pandemic to their advantage.[2]

Breaches by Type

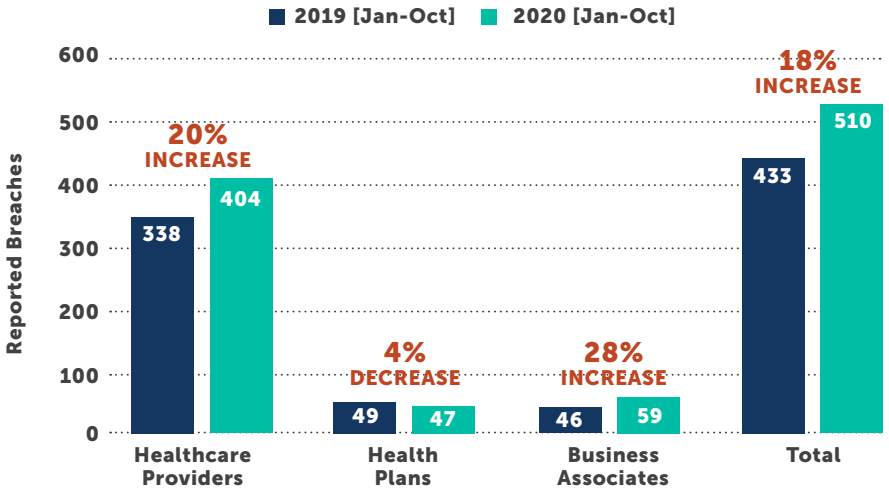


***The number of breaches for Jan-Oct 2019 was 435.**

Providers continue to be the most targeted sector, accounting for 79% of all reported breaches. Slightly more than 400 providers have been breached thus far this year, affecting just under 13.5 million patients. It's here we see most plainly the damage being inflicted by bad actors. As healthcare IT staffers work to deliver safe, secure work-from-home environments and telehealth visits, simultaneously, cybercriminals are ramping up phishing attacks to take advantage of the continuing healthcare crisis.

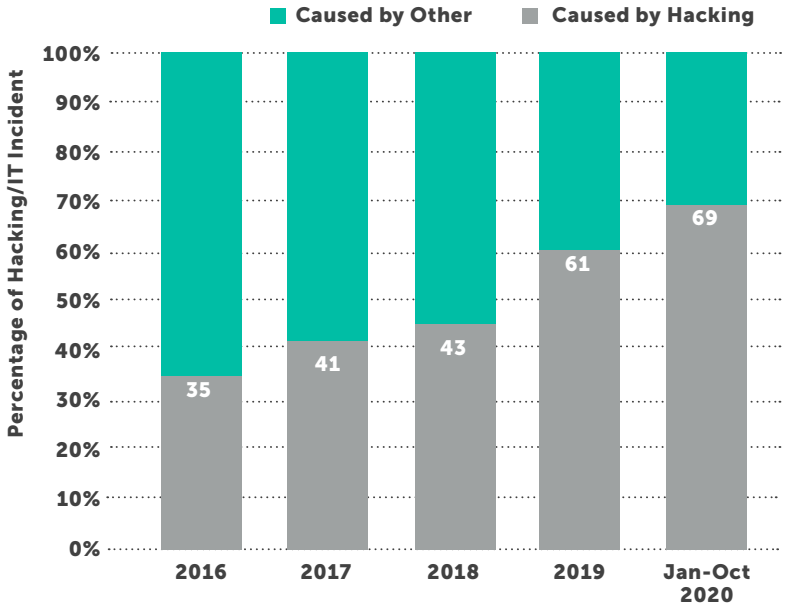
[1] Source: US Department of Health and Human Services Office for Civil Rights
[2] Source: https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-emerging-health-care-fraud-schemes-related-to-covid-19-pandemic

Entities Involved in a Breach



The shift to work from home and increase in telehealth use has taken a toll on overall security by creating an increased attack surface for cybercriminals. Malicious attackers or IT incidents remain the leading cause of breaches, rising 8% over the same period last year and causing 69% of all breaches. Unauthorized access is the second leading cause at 20%.

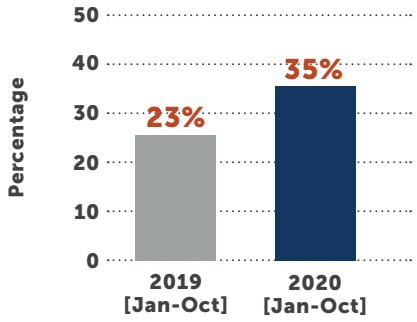
Breaches Caused by Hacking



Attacks on network servers are on the rise, increasing from 23% in January to October of 2019 to 35% in the same period in 2020. Ransomware attacks are still a major area of concern, with the FBI, Department of Health and Human Services, and Department of Homeland Security warning healthcare executives at the end of October about an imminent threat.[3] Government officials said a Russian cybercriminal gang planned to deploy ransomware to more than 400 healthcare facilities to create disruption in the sector, and several hospitals were subsequently attacked. Cybersecurity experts were not surprised that the government offered little mitigation advice beyond vulnerability patching on the October call.[4]

[3] Source: https://www.healthlawdiagnosis.com/2020/10/warning-to-hospitals-of-imminent-threat-released-by-u-s-government/
[4] Source: https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/

Attacks on Network Servers



Despite the attention given to ransomware attacks, email remains the most common attack vector used by those seeking to steal patient data. Phishing campaigns have proven so successful that they not only continue but grow more sophisticated and targeted. This serves as a strong reminder that end-user training and awareness must be at the top of any comprehensive cybersecurity program.

Despite the attention given to ransomware attacks, email remains the most common attack vector used by those seeking to steal patient data.

There was also a significant uptick in the number of breaches in which a business associate (BA) was involved in some way. From January to October 2019, the number of entities answering "yes" to "was a BA present" was 105. In 2020, it soared to 196. In great part, this was due to a massive ransomware attack in May on a cloud software company that is still causing ripples in the industry. One attack on a BA has a multiplier effect on health systems.

As we head into 2021, we see healthcare cybersecurity leaders overwhelmed with pandemic-related activities and budget difficulties. In too many cases, this leads to less-than-robust execution of day-to-day cybersecurity tasks. Our adversaries are clearly not easing up, so this is not the time to falter when it comes to taking a strong, risk-based approach to cybersecurity.

Pause to Consider

1. Have you made all necessary program adjustments to augment email security?
2. Are you executing an enhanced cybersecurity training and awareness program?
3. Is your organization's security program centered on risk mitigation?

OCR – Investigation & Fines

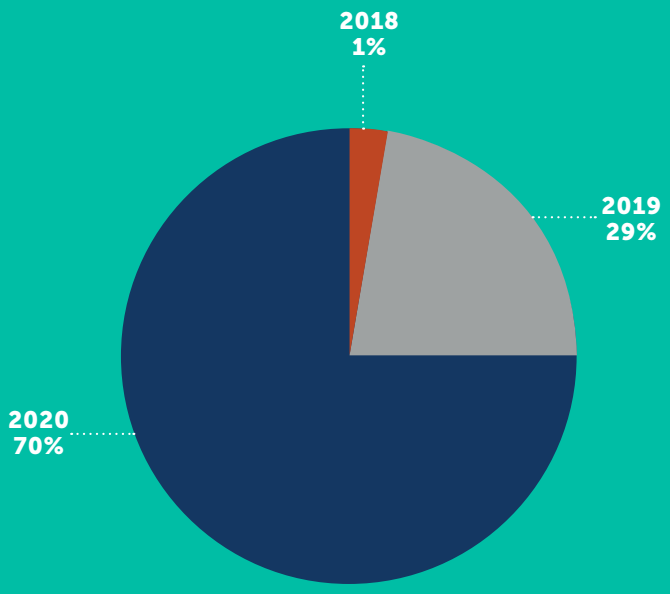
In the first 10 months of 2020, there were 11 resolution agreements reached between OCR and healthcare organizations. Each agreement included a steep fine, averaging just under $900,000 and a multi-year corrective action plan that required the organization to make improvements to its cybersecurity program.

According to HHS:

> *"A resolution agreement is a settlement agreement signed by HHS and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement may include the payment of a resolution amount."*

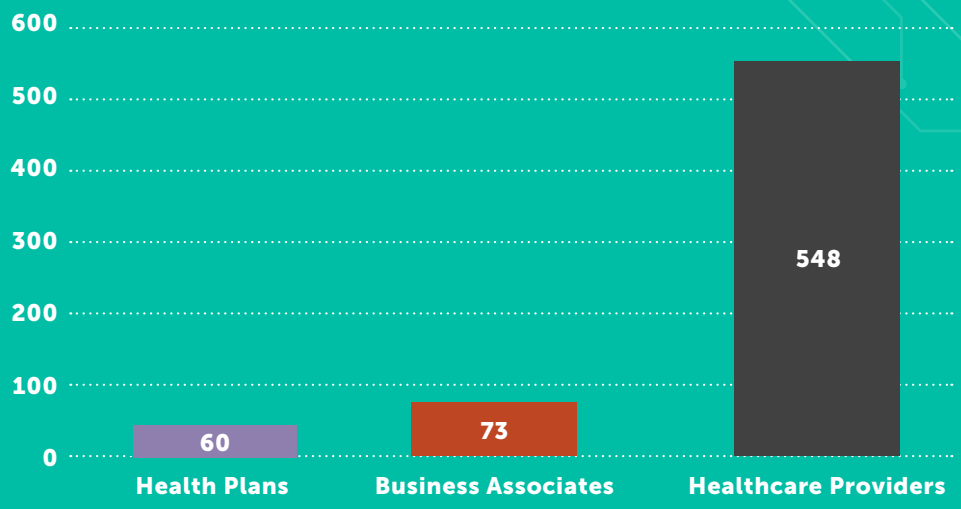
Prior to a resolution agreement, a multi-year investigation takes place, costing organizations time and resources. Currently, there are 683 organizations under investigation for incidents dating back to 2018.

Percentage of Organizations Still Under Investigation by Date of Reported Breaches



It's difficult to state the toll a breach followed by an OCR investigation takes on a healthcare organization. Both the initial breach and resulting investigation are incredibly time consuming, causing strategic planning and new-project implementation to slow or stop completely. The possibility of that scenario can be greatly reduced through an annual risk assessment followed by strict attention to a corrective action plan. Healthcare IT and cybersecurity executives who implement a disciplined, documented, risk-based approach not only reduce the likelihood of an incident occurring, they set themselves up for success should they find themselves working with OCR.

Entities Under Investigation



Pause to Consider

1. Are you documenting progress against your corrective action plan?
2. How does your organization track real progress against corrective action plans?
3. Are you taking a risk-based approach to capital allocation within your cybersecurity budget?

2020 Market Dynamics

While the global pandemic dominated headlines across industries, healthcare organizations specifically faced these four market forces, which will reverberate for years across hospitals and health systems:

1

Incident Response Plans

Cyberattacks on healthcare organizations did not abate during the pandemic. IT staff also had to deal with an explosion of telehealth services and moving non-clinical employers to work-at-home environments, increasing the attack surface and creating the need for more complex incident response plans.

2

Tools Rationalization

The time has finally arrived for healthcare IT departments and cybersecurity teams to fully understand their technology spend, rather than using technical point solutions that overlap with other products or create security gaps.

3

New Ways to Work

The pandemic has forced IT and cybersecurity leaders to assess the state of their human capital, recognizing that not all cybersecurity employees need to report to the office and to explore the idea of outsourcing cybersecurity monitoring and other cybersecurity functions.

4

Security Beyond the Walls of the Hospital

Enabling work-from-home brought new threats and technology challenges to healthcare organizations and increased the attack surface, underlining the importance of real-time network monitoring and staff training against phishing attacks.

Get Your Incident Response Plan in Order

An incident response (IR) plan is much like disability insurance — you have to have it, but you hope you'll never need it. The pandemic pushed two issues to the forefront that likely brought the need for a comprehensive IR plan into sharp focus: spinning up telehealth services to serve patients remotely and surmounting the cybersecurity challenges related to moving non-clinical workers to remote environments. Couple this with the continuously increasing cyber threat landscape, and if you haven't given your IR plan much thought or dusted it off lately, now is definitely the time.

Cybercriminals have been busy during the pandemic, and many specifically target healthcare organizations because of the heightened value of medical records. Should an incident occur, you need to know immediately who's in charge, whom to contact, what to do, and in what order. Right now, before an attack has occurred, is the time to carefully think through and construct you IR plan. Then, should an incident occur, your organization will have a critical tool already in place to minimize the damage. Creating an IR plan on the fly, under the pressure of an attack, is a losing proposition. That's why a current IR plan is critical, to provide the necessary guidance and structure at a time of crisis.

> If your IR plan is one page or was downloaded from the internet with the names changed to your hospital, you really don't have a plan.

Depending on the incident, the difference between activating a well-designed IR plan and suddenly recognizing that yours is insufficient could cost you several days, if not weeks, in downtime that no hospital or its patients can afford. Knowing what to do during a ransomware attack, for example, could mitigate the threat quickly and preserve vital forensic evidence that can help identify the perpetrators and be useful during the cyber insurance claim process.

An incident response plan must contain an accurate inventory of all the technology connected to your network, not just the EMR and the radiology system but the connected HVAC controls, the drink machine that takes credit cards — everything. Major cybersecurity incidents have occurred through a breach in an ancillary system.

There are likely many connected devices you don't exercise direct control over, such as biomedical devices. If you can't control a connection or a device, segment those connections away from the mission-critical systems.

The IR plan must also include those who need to be contacted, and in what order, when an incident is detected. If you have either an internal computer security incident response team (CSIRT) or a security incident response team (SIRT), that's probably your first call. If you outsource system monitoring, your managed security service provider (MSSP) likely alerted you to the incident and is prepared to deploy security tools and incident response utilities to investigate the incident further.

The appropriate executives to notify depend on the reporting structure of the IT and cybersecurity department. If necessary, the legal team and cyber insurance carrier should also be contacted.

Containing the threat from spreading to additional systems and eradicating it are top priorities. If a forensics team is involved, make sure any evidence is preserved. This step is critical and must not be overlooked. Once the system is cleaned and evidence is properly preserved, the affected system can be rebuilt and put back on the network, which typically occurs in chunks and through the efforts of multiple teams who are tackling certain areas in a predetermined manner.

In a larger scale response, it's common for several dozen people to be involved: a combination of in-house staff, outsourcing vendors, third-party vendors with assets on the network, forensics team, insurance company, general counsels, and senior leadership. If you're using an MSSP for any security services, make sure the service-level agreement (SLA) includes timing for an in-person response, if necessary.

The incident isn't concluded when the final system is cleaned and returned to the network. That only occurs following a lessons-learned phase to better understand what went right, what went wrong, how it went wrong, the root cause, performance of the respondents, and much more. Breathe a sigh of relief that the crisis has passed, but recognize that understanding the previous incident can help your organization plan better for the next incident.

In addition to an IR plan, hospitals also need a complete implementation of security controls and utilities. For example, the forensics team may need firewall logs for the month preceding an incident. Who is responsible for maintaining them, and where are they kept? You may have a security information and event management (SIEM) vendor or outsource monitoring and/or the service desk. You must make sure you fully understand what services are being provided — and, just as important, what services for which you are responsible. It may make sense to consider an IR retainer and conduct an annual tabletop exercise to help make sure you are prepared.

An IR plan isn't a one-and-done process. Rather, it's a living document that should be constantly updated and practiced from time to time. Incidents can cause critical impacts when it comes to a hospital's ability in ensuring that patient safety and care is handled appropriately. In the healthcare cybersecurity landscape, the order of impact importance to conquer are availability, integrity, and confidentiality. Caregivers require that their systems are available, and that data integrity is maintained when providing care. Rapid and appropriate response to an incident is key in mitigating these impacts.

In the healthcare cybersecurity landscape, the order of impact importance to conquer is availability, integrity, and confidentiality.

Pause to Consider

1. Does your organization have an incident response plan?
2. When was the last time incident response plan was updated and tested?
3. Have you completely implemented security controls and tools?

Tools Rationalization: Do You Have More Software than You Need?

If your organization is buying technical point solutions, you may not have sufficient security coverage, and it's quite likely that you're paying too much for this reduced coverage. While the concept of tools rationalization and gap analysis is not new, the idea is gaining ground as software becomes more robust and the industry moves from a perpetual license model to one that is subscription-based and often software-as-a-service (SaaS).

Much like an organization needs an inventory of the assets connected to its networks, hospitals also need to understand what cybersecurity technology they have, what it covers, who is responsible for maintenance/monitoring, what type of software it is (purchase/subscription), and when any renewals occur. For the tools you have, you must define their capabilities and determine whether there are unused capabilities that some other tool is providing. Think about whether there is a consolidation opportunity with tools that may be providing the same or similar functionality, or are targeted at the same or similar outcomes? Which ones are best-in-class? Are there specific tools that are nearing end of life or aren't being supported any longer?

While right-sizing your technology toolkit is important, you also must consider whether new tools on the market could (or should) replace several tools you already have. Across the solution spectrum, technology continues to evolve to the point that a consolidated, purpose built tool may effectively handle several tasks, compared to a few years ago when companies acquired point solutions for individual tasks.

Technology fatigue can create significant issues, as can lack of sufficient staff to appropriately maintain and monitor these tools. Even the largest healthcare technology and cybersecurity departments struggle with staffing, as one engineer manages four or five technical solutions — some of which may not be within the engineer's realm of expertise. A comprehensive review of your technology can uncover gaps, overlaps, and instances where software isn't being used to its full capacity.

Make note of when subscriptions expire and of any contractual price increases. Most subscription-based software is continually upgraded and enhanced, which can justify the price hikes. But as functionality increases, the utility of other software you're using may decrease.

Another important consideration is whether the software you have is being used to its fullest extent. During the sales process, a demonstration likely showed the entire range of features, but not all of them may have been compatible with your particular software mix, you may have been using conflicting solutions, or IT didn't sufficiently mature the software during implementation. In many cases, software is deployed and implemented with vanilla out-of-the-box configurations, without proper architecture or planning.

Organizations often recognize a small percentage of functionality from these deployments while primary, more advanced functionality is missed, leaving you more vulnerable than you think.

To counteract this issue, understand and document your goals and specify the maturity point you want to achieve. Continuously measure progress and bring relevant stakeholders together on a regular cadence to provide updates, receive feedback, and discuss any issues.

Meetings will become less frequent as the software matures. But remember that software implementation is a journey and not a destination, especially as vendors continually upgrade and improve their offerings.

When evaluating cybersecurity technologies, hospitals and health system staff should first understand what software they have, what they can do with their existing platforms, where the gaps are, and how new software will fit within the IT infrastructure. Characteristics such as "best," "cheapest," "most versatile," and others must be evaluated against existing software, budget, and the staff's capacity to effectively manage. Take antivirus software, for example. An IT engineer probably wants the solution that flags the most anomalies.

The IT executive will look at the technology, its price, and how easy/difficult it is to manage. If Software A catches 99.9% of bugs, and Software B catches 98% but is half the price and easier to manage, which one should a company choose? Compatibility with other technical solutions and vendor satisfaction are other important considerations. If Product A catches slightly fewer issues but fully integrates with other company products already deployed, Product A may be the better option, especially if you're satisfied with the current vendor relationship.

Furthermore, since Product A integrates with other technologies you already own and manage, you may reduce risk further versus options that do not integrate.
The initial assessment can take time and diligence to ensure all products are included, but the process will become easier in subsequent years. Right-sizing your technology spend can reduce the coverage gaps among your software and help ensure you are using your technology to its fullest extent.

Pause to Consider

1. Have you performed a tools rationalization exercise?
2. Do you have cybersecurity tools that are redundant and/or underutilized within your organization?
3. Do you know how your current technology controls compare with other solutions in their category?
4. Have you aligned your installed cybersecurity solutions with your security program and changing business requirements?
5. When is the last time you had a feature review/strategic roadmap discussion with the manufacturers of your solutions?

New Ways to Work During the Pandemic and Beyond

The global pandemic has fundamentally changed healthcare cybersecurity and how it's delivered. Those changes have clarified the role that security plays in IT and throughout organizations. Many non-patient facing employees, such as those in IT, started working from home as the nation shut down in March and will continue to work remotely for the foreseeable future. Some of those workers may never return to a physical campus, as the capability of working remotely has quickly moved from nice-to-have to mission-critical.

Sheer will and heroic efforts among IT staff made possible the shift to remote working and the delivery of new telehealth services almost overnight as providers kept the connection to patients any way they could. Remote working brings new security and compliance challenges though, and telehealth connections must be kept secure.

Besides the obvious challenges that COVID-19 brought, the pandemic also forced hospitals and health systems to look closely at their technology and IT staffing models. In healthcare, protecting IT infrastructure is typically not a core competency. Of course, maintaining system availability, ensuring data keeps flowing, and patient and operational data remain secure are primary objectives, but the pandemic brought to the forefront the recognition that not all IT and cybersecurity functions need to be handled in-house.

A few years ago, moving on-premise systems to the cloud was unthinkable among many provider organizations. As SaaS offerings became the norm across customer platforms and most other industries, healthcare slowly caught onto the idea, now viewing SaaS as a way to efficiently deliver services while reducing the IT maintenance burden. Similarly, healthcare is now warming to the use of remote or outsourced IT and cybersecurity staff to fill roles within the organization, everything from server maintenance and routine monitoring to senior technology and security roles. While complete IT and cybersecurity outsourcing may become a trend in a few years, any steps in that direction will be cautious and deliberate.

Cybersecurity staffing is an ongoing challenge for all industries. An association of cybersecurity professionals estimates that the United States needs an additional 500,000 cybersecurity workers to handle current demand. Another survey shows that seven in 10 companies report worker shortages and that 45% say this shortage has gotten worse in recent years.[5] Hiring qualified cybersecurity staff in healthcare can be a particular challenge, depending on geography, department composition, and opportunities for advancement. Some hospitals report difficulty hiring entry-level cybersecurity workers to perform basic monitoring and maintenance tasks, while others say that CIOs and CISOs are hard to hire.

[5] Source: https://www.cnbc.com/2020/09/05/cyber-security-workers-in-demand.html

An association of cybersecurity professionals estimates that the United States needs an additional 500,000 cybersecurity workers to handle current demand.

The surge of teleworking has opened the eyes of many healthcare leaders, who now recognize that IT and cybersecurity staff aren't required to live within a small radius of the hospital. But hospitals and health systems are competing for talent nationwide and against specialized managed security service providers (MSSPs) that can offer a greater depth and a variety of cybersecurity experiences over what hospitals are able to offer.

The answer for many healthcare organizations will be a hybrid model, where some security and maintenance functions are handled by MSSPs while some core functions remain in-house. A hybrid model also allows organizations to bring a best-in-breed approach to cybersecurity, gaining expertise and best practices from across the MSSP's clientele. In terms of monitoring, for example, a cybersecurity provider with healthcare expertise can spot a potential attack when it first occurs, warning other hospitals that it serves to be prepared or taking proactive steps to protect those systems.

Regardless of the staffing model, organizations must have standard operating procedures in place that are followed consistently and a clear line of authority that's triggered when significant events occur. The pandemic should have served as a wake-up call to organizations that did not have current or updated business continuity or incident response plans in place. Almost overnight, outpatient visits and elective surgical procedures ceased, and many employees were forced into working from home – if the hospitals and health systems could support that. Some on-premise IT systems couldn't be accessed remotely, or there weren't sufficient assets to allow those who could perform their jobs at home to do so. Organizations that prepared and had alternative working plans fared much better than those that were left scrambling.

Having a clear line of authority from the server room to the C-suite is also critical. In smaller organizations, IT decisions may rest with the CEO, the COO or the chief legal officer. Larger organizations have dedicated IT executives, such as a CIO, CTO or a CISO, but sometimes IT and cybersecurity reporting is split between IT and compliance. The key is to understand how the reporting works before an incident occurs.

Don't let the pandemic fade into memory before thoroughly examining your staffing, your operating procedures and your ability to react quickly and decisively if your organization is compromised.

Pause to Consider

1. Is it getting harder to hire/retain competent cybersecurity staff?
2. Is your IT and cybersecurity staffing model working for your organization?
3. Are there clear lines of authority/notification should an IT incident occur?

2020: The Year Data Escaped Hospital Defenses

Hospitals and health systems overall have done a fairly decent job protecting data within the four walls of the facility, keeping the marauders at the gate, if you will. But the pandemic has thrown open the gates of the castle, leaving data exposed in isolated homes where workers decamped when the pandemic hit and forcing hospitals to rethink data governance in this new paradigm. Rather than defending a central system, facilities are now fighting the data security war on multiple fronts.

Taking the castle analogy a step further, people have always been the weak link in the defense system, using poor passwords, writing passwords down, clicking on suspicious emails or even deliberately sabotaging security. Recent cyberattacks include bogus emails from the U.S. Department of Health and Human Services targeting the C-suite for COVID-19 info and malicious links contained within Google docs.[6]

The quick change in working environment for non-clinical staff has exposed additional vulnerabilities that hospitals are trying to close by gaining greater visibility to new endpoints, adding encryption and user access management and increasing user training and data governance through careful and timely examinations of user logs. Cybercriminals are also getting more sophisticated, so healthcare cybersecurity teams must keep pace even to maintain a security status quo.

Many data security best practices have been around for years, such as those requiring strong passwords and changing them frequently, but any best practice must be adhered to in order to remain effective.

Best practice for remote work is to provide a company-supported laptop equipped with appropriate security controls. But many hospitals didn't have sufficient laptops to support everyone working from home. Some employees took their company desktops home, while many others logged in remotely using their personal computers and firewalls. Bring Your Own Device (BYOD) policies limit hospital control over the machines and provide limited visibility unless effectively managed.

From a cybersecurity fundamentals perspective, near real-time monitoring of security information and event management (SIEM) software should be a priority. SIEM software collects data from throughout the technology infrastructure, monitors and analyzes information for possible security risks enabling organizations to take action against any threats.

SIEM monitoring can be performed in-house, but partnering with an outside company may be the right option if you want 24/7/365 threat visibility and protection. One such check that can be performed is the "impossible traveler," where a single user is logged in from outside the United States or from two different, widely separated locations at the same time.

Network geofencing can prevent many such intrusions by locking the system down to specific areas, states or countries. Another warning sign could be users forwarding emails to an account outside the company domain.

[6] Source: https://www.healthcareitnews.com/news/hospitals-said-tighten-email-security-response-ceo-spear-phishing-attempts

But many intrusions can be prevented by sound data governance and strong user training that's repeated frequently. Proper identity and access management programs along with practicing least privilege access can limit information to those in certain departments or with certain job functions, narrowing the universe of users. Billing staff, for example, may not need access to the general ledger system in order to perform their jobs. Another protocol could disallow the downloading of files onto local devices and removable media. Also, many users may not need email to perform their job function, although culturally they may have always had company provided email.

The biggest security risk continues to be employees who do not practice proper email hygiene when opening and responding to emails. Many of the security tips are basic, but they warrant repeating. Automatically scan incoming emails and attachments for malicious content. Place a warning banner on all emails originating outside the health system to remind users this is an external email. Require strong passwords that are changed frequently. Use multifactor authentication. The latter can be expensive for smaller health systems, but there are other ways to lock down software.

Some hospitals, for example, have discovered that not every worker actually needs email, saving money on user licenses while tightening security. Non-management nurses may need email once a year for compliance training. Otherwise, they use public access computers where their ID badge serves as the login credential that allows access to online versions of software within the facility's information security infrastructure.

Above all, awareness and training must highlight the importance of treating every email and every attachment as a potential threat. While working from home, it would be easy to click on an email that looks like it's coming from a boss or from the health system, perhaps a meeting reminder with an attached agenda to review.

As security threats evolve and become more sophisticated, health systems must keep up. The failure to adapt and invest in cybersecurity may lead to an unexpected interruption of patient care. Furthermore, it could also mean an expensive data breach, with not only the potential for a large fine but the prospect of a costly remediation process and loss of reputation in the market. It's a risk that hospitals and health systems cannot afford.

Pause to Consider

1. Do your data protection policies reflect how people are actually working?
2. Is near real-time monitoring of security information and event management (SIEM) software a priority?
3. Are you conducting regularly scheduled employee awareness and training on IT security protocols?

Were We Right?

A Look at Fortified's 2020 Predictions

Prediction

Double-Digit Increase in Breaches: Healthcare will experience a 10-15% increase in the number of entities breached over 2019, with providers being the most targeted and exploited segment.

So how did we do?

Through the first 10 months of 2020, the number of reported breaches increased 18% over the same period in 2019. Also as expected, provider organizations were the target 79% of the time, the 11th straight year for this dubious honor.[7]

Prediction

Continued Cybersecurity Technology Vendor Investment and Consolidation: Given the amount of investment and focus on threats related to IoT, further consolidation in IoT cybersecurity is expected.

So how did we do?

Numerous IoT and medical device organizations raised additional capital including Ordr in March and Medigate in September 2020.

Prediction

Email as the Attack Vector of Choice: As in prior years, bad actors will continue to use sophisticated phishing campaigns to target and exploit healthcare organizations.

So how did we do?

Despite the attention paid to ransomware attacks, email remains the most common attack vector used by those seeking to steal patient data, representing 38% of all attacks. Phishing campaigns grow more sophisticated and targeted, demonstrating the need for ongoing user training.[8]

Prediction

Investment in Advanced Endpoint Technologies: Healthcare organizations will make additional investments in endpoint security technologies to secure the threat landscape at the edge. Remember to consider how your organization will operationalize this technology to extract the most value and maximize protection.

So how did we do?

Endpoint security, indeed, came to the forefront in 2020, led in large part by the fundamental shift of employees to remote working and an increased reliance on telehealth visits when hospitals and clinics shut down during the early spring. To protect those endpoints, organizations are making investments in endpoint detection and response (EDR) technology and managed detection response (MDR) services as a supplement to traditional security information and event management (SIEM) services.

[7] US Department of Health and Human Services Office for Civil Rights
[8] Ibid.

Cybersecurity Outlook 2021

Double-Digit Increase in Breaches

Healthcare would like to stop this streak of double-digit growth in data breaches, but 2021 won't be that year. Until the industry commits firmly to cybersecurity strategic roadmap services, expect this unfortunate trend to continue, fueled by email phishing and ransomware attacks.

Larger Spend on Cybersecurity

The industry has started to recognize that cybersecurity spending must expand to match the rising number of threats as well as threat surface areas which have dramatically increased with more health systems relying on externally facing services. As a result, the number of endpoints has also increased as the growing demand for telehealth services and remote workforce requirements are met. The C-suite has recognized and prioritized these high value risks, which means purse strings likely will loosen. Spending may be on services and software however, rather than human capital.

Focus on Verifying Credentials and Access

Organizations will continue to move toward tighter access security, including multi-factor authentication (MFA), zero trust, identity access management (IAM) and cloud access security brokers (CASB) applications in an attempt to better control authorized access to data and systems. The number of healthcare organizations building programs and governance in these areas will increase significantly, many in a "crawl, walk, run" method.

The Advent of Tools Rationalization

IT departments are finally looking around and asking fundamental questions, such as "Why do we have all this software?" The reasons for tools rationalization include identifying and eliminating security gaps, reducing expenses, and ensuring best-in-class software is being deployed. Significant personnel and technology savings can be recognized as a result, as well as increased effectiveness of security controls.

Moving Forward

Understand Primary Threats

Email phishing remains the No. 1 threat to networks, so user training remains critical. Additionally, IT departments and cybersecurity teams should stay current on potential threats and review/test incident response plans.

Update, Monitor, and Test

The availability and integrity of your network and connected systems are critical. Ensure systems, software and end-point security tools are up-to-date, monitor diligently for threats, and test your backup/downtime plans.

Get Strategic about Security

Beyond day-to-day security tasks, monitor and identify threats to your organization and environment. Based on those threats, develop plans to mitigate or remediate them. This can be accomplished by assessing your current security technologies to ensure they are fully operationalized and reviewing the processes and policies these technologies support. Additionally, identify tools, processes, and policies needed to mitigate any gaps identified. Update and rehearse your IR plan.

Go Beyond the Basics

Visibility and identity are key areas of concern when looking at the maturity and effectiveness of a security program. A couple of areas which make significant strides in an organization's security posture are deploying advanced end-point protection and/or managed detection and response (MDR), disabling unused or unnecessary accounts and end points. Taking a hard look at identity and access management (IAM) controls to include enabling multi-factor authentication (MFA) on externally exposed services is key to reducing an organization's threat surface area.

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 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. 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®

fortifiedhealthcaresecurity.com