Fortified HEALTH SECURITY

2022 Horizon Report

The State of Cybersecurity in Healthcare

CEO's Message

One in eight men, women and children in the United States — 13% of the populace. Patient information on 45 million people in the U.S. was reported as breached to the Office for Civil Rights (OCR) in 2021.[1] Some people's information was likely breached more than once, but the overarching point is that more than 700 reported breaches is far too many.

Between breaches and an increasing number of ransomware attacks, federal and state regulatory agencies and cyber insurance companies are taking notice, adopting comprehensive cybersecurity policies and procedures that increase compliance and mitigation costs. The healthcare IT and security footprint will never return to just the hospital's four walls. Born out of necessity during the pandemic shutdown in March 2020, remote work or hybrid work is here to stay for many healthcare workers, which makes cybersecurity more critical.

Healthcare cybersecurity is at an inflection point, similar to what the payments industry faced in 2004 amid rising instances of fraud. Major credit card issuers came together to create a common set of security standards that merchants and payment processing organizations had to follow.[2] This level of industry-wide cooperation won't be as easy to institute in healthcare, but the status quo is no longer acceptable.

There have been many headlines about healthcare organizations that are facing their cybersecurity challenges openly, sharing how a massive ransomware attack resulted in weeks of pen-and paper medicine while the EHR was offline. This has led many healthcare organizations to understand that investing in cybersecurity is necessary to stay open and take care of patients and the community, which is their ultimate mission.[3]

"Born out of necessity during the pandemic shutdown in March 2020, remote work or hybrid work is here to stay for many healthcare workers, which makes cybersecurity more critical."

We're hearing similar openness during Fortified's monthly roundtables and webinars, where cybersecurity professionals come together to share stories, learn from each other and seek advice. There is no hidden agenda, just an opportunity to bring the industry together to discuss common issues.

One large challenge the industry faces is rising IT cybersecurity salaries and the ongoing shortage of qualified workers. When workers are leaving for salary raises that top $50,000, healthcare organizations must honestly assess whether they can afford to keep all aspects of IT security in-house. Hackers never sleep, so 24/7 monitoring is critical. Is that a function your organization can afford to perform on its own?

A recent survey of healthcare IT and IS executives showed that only 11% said cybersecurity was a high priority spend and two-thirds did not track return on investment for cybersecurity spending. At the same time, half of respondents said their organizations had been forced to shutter operations in the previous six months due to a cyber incident.[4]

Hospitals and health systems simply must do better, and it is my hope that the Horizon Report builds awareness about the cybersecurity landscape in healthcare and provides valuable insight for your program. We welcome your feedback and perspective at: horizonreport@fortifiedhealthsecurity.com. Enjoy.

Regards,

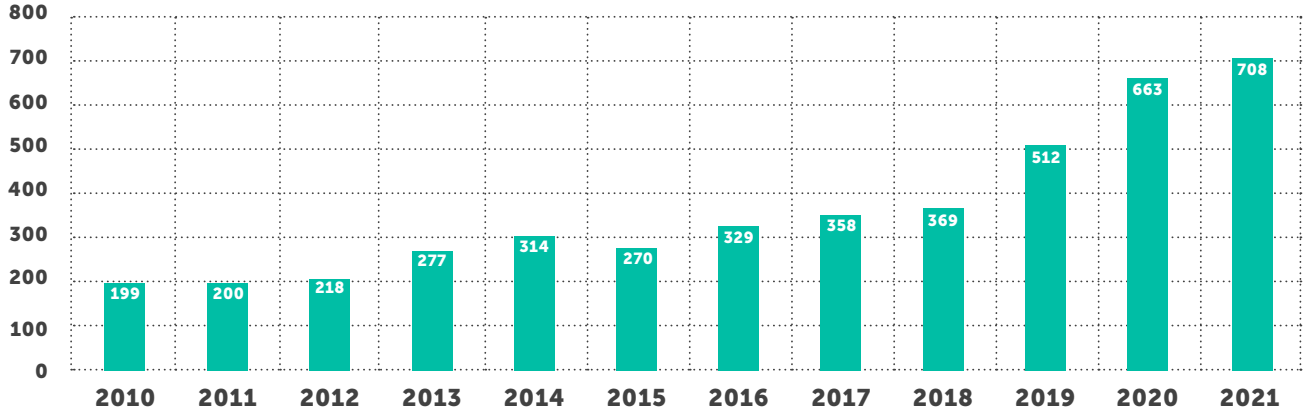
Dan L. Dodson

[1] Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[2] Source: https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/pci-dss-history-everything-you-need-to-know#:~:text=The%20history%20of%20PCI%2DDSS,DSS%201.0%20in%20December%202004
[3] Source: https://www.beckershospitalreview.com/finance/scripps-records-q3-operating-loss-notes-cyberattack-cost-of-112-7m.html
[4] Source: https://healthitsecurity.com/news/cybersecurity-vulnerabilities-not-priorities-for-most-hospitals

2021 Year in Review

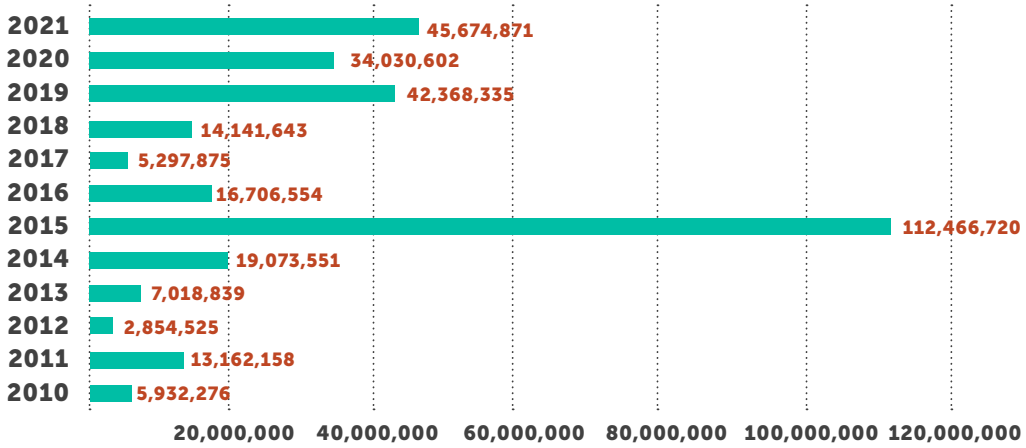
While 2021 might be seen as a year of recovery following a tumultuous pandemic-dominated 2020, cybercriminals continued to target providers, health plans and their business associates. In 2021, over 700 healthcare organizations reported a breach of 500+ patient records to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights, the so-called "Wall of Shame." As we expected, this set another unfortunate record as the highest number of breaches in a year. [5]

Breach Totals by Year



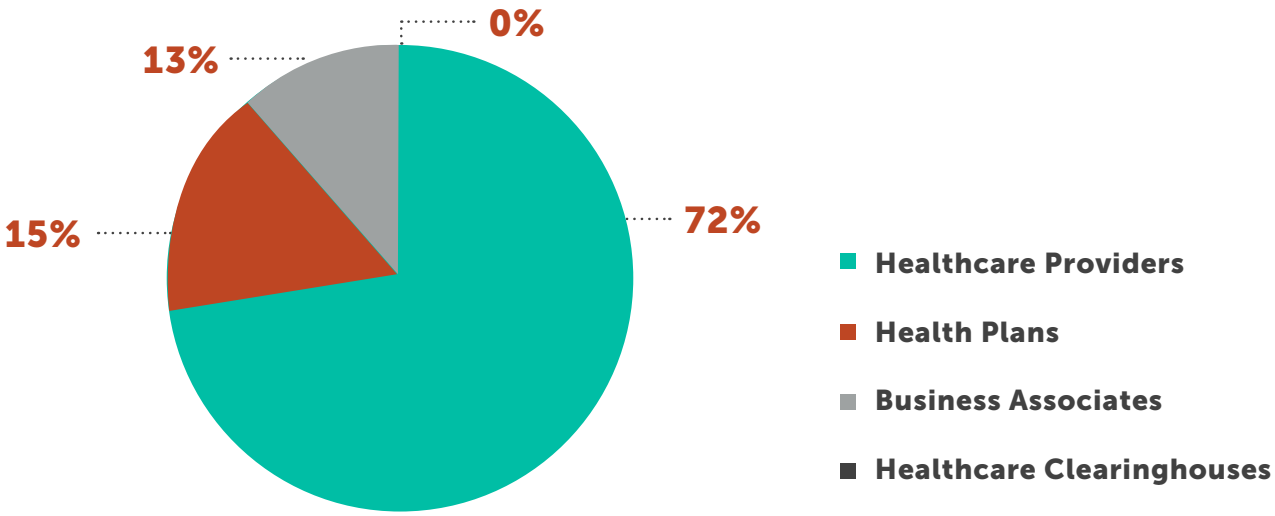
Through 2021, the number of reported breaches increased 6.7% compared to the same period last year. However, the total number of breached records increased by 34% from 34 million in 2020 to close to 46 million in 2021. This is the highest number of individuals affected in a single year, with the exception of 2015 when two major breaches from Anthem Inc. and Premera Blue Cross alone affected nearly 90 million individuals.

Individuals Affected by Year



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

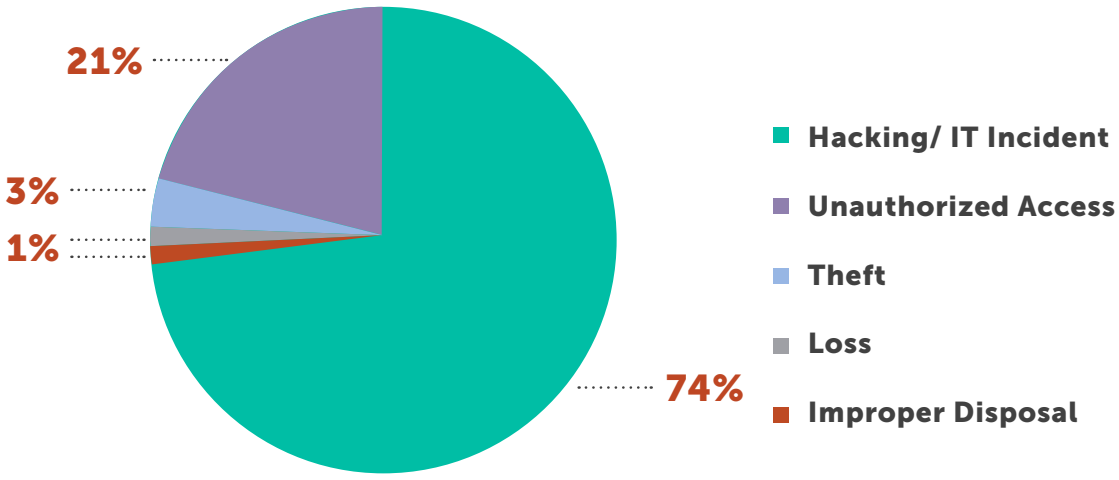
Type of Entity Reporting the Breach in 2021



Healthcare providers remain the overwhelming source of breaches, accounting for 72% of all incidents. Just over 500 providers have reported breaches in 2021, affecting over 28 million patients. Health plans reported 15% of all breaches, with nearly 7 million affected members. Business associate breaches represented 13% of the total number and more than 10.5 million patients.[6]

Hacking incidents on healthcare continue to increase year-after-year. As late as 2018, hacking represented under 50% of all cybersecurity incidents. Hacking was cited in 522 incidents in 2021, 74% of total incidents. Unauthorized access is the second-leading cause, cited in 21% of all incidents.

Type of Breach in 2021



The sheer number of technologies connected in a modern healthcare ecosystem remains an area for concern as bad actors try to find the path of least resistance to maliciously access a network. Often, sources of entry can seem innocuous, such as heating and air technologies, pneumatic tube systems in hospitals or one of the estimated 430 million Internet of Medical Things (IoMT) devices used around the globe.

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

More than half of IT professionals said they are concerned about building system technologies and electrical devices being used as an entry point, followed by imaging devices, equipment that dispenses medications, check-in kiosks and equipment that monitors vital signs. Not all the news is discouraging, with 86% of healthcare IT professionals saying their organization has hired a CISO and 95% indicating their connected devices had the latest software.[7]

In 2021, email attacks have taken a back seat to network server attacks that accounted for 53% of all incidents in 2021. Email attacks comprised 27% of the total.[8] These statistics mirror those in other industries that are reporting record numbers of ransomware attacks.

For healthcare IT professionals, the data above clearly shows that attacks continue throughout the technology infrastructure, from phishing and vishing campaigns against workers to direct attacks on networks to inflitration via business associates.

As 2022 dawns, healthcare cybersecurity leaders face a multifaceted war on IT systems that shows no sign of letting up. Turning the tide starts with a strong, risk-based approach to cybersecurity.

Pause to Consider

1. Has your organization identified its cybersecurity weak points?
2. What actionable steps are you taking to mitigate those risks?
3. Is your organization's security program centered on proactive risk mitigation?

[7] Source: https://www.zdnet.com/article/healthcare-security-it-pros-warn-of-vulnerable-hvac-systems-imaging-machines-check-in-kiosks-and-more/
[8] Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

2022 Market Dynamics

Although the pandemic continues to dominate headlines for the nation's hospitals and health systems, these four issues require focused attention and monitoring because of the potential to upend healthcare cybersecurity.

1

Cyber Insurance
Cyber insurance is changing fast, with insurers taking an increasingly critical view of the current threat landscape, policies, coverages and deductibles. Know what your policy covers (and what it doesn't), what security measures you have in place, and whether you can actually attest to the policy requirements.

2

Government Regulatory Changes
Healthcare, again, has the dubious distinction of taking the longest to identify breaches and spending the most money on remediation. The government has taken notice, with a plethora of new regulations and guidance related to cybersecurity.[9]

3

Disruptions to Patient Care
Rampant ransomware and its potential to disrupt patient care are driving healthcare organizations to raise the cybersecurity bar. Doing nothing isn't an option, but the costs for in-house security monitoring can be quite expensive.

4

Identity and Access
Microsegmentation and multi-factor authentication (MFA) initiatives represent a middle ground between a wide-open network and the zero trust model, which requires identity validation before granting access to any system. Grouping assets by function or ring-fencing critical and sensitive data can help decrease the likelihood of a negative impact.

[9] Source: https://www.reuters.com/legal/legalindustry/cybersecurity-data-privacy-foresight-2022-2022-01-21/

Cyber Insurance: What to Know Before Renewal

With malware attacks proliferating and no end in sight, cyber insurance sales have skyrocketed. Since 2016, the uptake for cyber insurance has doubled among healthcare organizations, with much of that growth occurring during the pandemic.[10]

Cyber insurance is intended to protect organizations against the fallout from cyberattacks, covering the financial burden associated with security incidents. It might sound like a good idea, but a growing number of critics claim that cyber insurance actually incentivizes criminals, because ransomware victims can skimp on security measures and simply pay the ransom demand, which will then be covered by insurers.

Having cyber insurance doesn't take the place of a strong cybersecurity infrastructure. Increasingly sophisticated attacks continue with larger payouts that make obtaining cyber insurance more difficult — and more expensive. Insurance companies are demanding more rigorous attestations and taking additional steps to ensure minimum security standards are met.

"Having cyber insurance doesn't take the place of a strong cybersecurity infrastructure."

Remember, if you don't comply with the terms of the policy, you may not be truly covered during a time of need.

If your insurer requires an endpoint detection and response (EDR) solution or other technology, policy terms dictate those systems must be fully operational before a claim is paid. Insurers have done their ROI analysis and know that health systems with EDR solutions, for example, are much less likely to pay out through reduced risk. Expect a much bigger push from your cyber insurance for health facilities to deploy specific security technology in the next year or face reduced or declined coverage.

In many ways, healthcare and cyber insurance are at the same point that financial services and retailers were 10 to 15 years ago. At that time, cybercriminals targeted retail, banking and financial sectors almost exclusively for credit card data. These companies weren't spending enough on cybersecurity protection mechanisms — people, processes and technology — to safeguard that data.

Changes didn't occur until the organizations dealing with the associated fraud created Payment Card Industry Data Security Standards (PCI DSS) and a Payment Card Industry Council. These efforts enabled the payment card industry to manage the risk and ultimately transfer liability back to the merchants who process credit cards.

[10] Source: https://www.zdnet.com/article/cyber-insurance-premiums-take-up-rates-surge-says-gao/

Increasingly, cyber insurance policies are putting more risk onto covered entities, and some insurers are exiting the healthcare industry. In addition to higher premiums, coverage reductions and per-incident caps, insurance providers are conducting more thorough annual reviews to determine an organization's current state of security before renewal. These reviews can include lengthy attestations that ask about specific vulnerabilities, such as SolarWinds or Microsoft Exchange vulnerabilities. These are major vulnerabilities in the IT world at large, not just healthcare.

Cyber insurance companies are asking for specific documentation and attestations that health systems have checked their security environment and whether the organization can confirm they have remediated or mitigated identified risks. In addition, cyber insurers are requiring longer self-assessments with answers to questions, including:

+ Do you have a third-party risk management program?
+ Have you implemented multi-factor authentication?
+ Do you have endpoint detection?
+ Do you have centralized logging?

Insurers are looking for the core security technologies that indicate hospitals and health systems are prepared to identify, respond to, and contain cyberattacks.

Healthcare organizations face sharper scrutiny on the regulatory front as well. In addition to direct financial impact, cyberattacks can bring Office for Civil Rights (OCR) fines if patient data is compromised. State and federal agencies are putting the responsibility on healthcare providers to ensure that sensitive data is reasonably protected. When a ransomware attack does strike, health systems that pay ransom to get data back may run afoul of U.S. Treasury Department rules regarding foreign actors.[11]

Healthcare cybersecurity spending still lags most other industries, but there might be faint light at the end of the cybersecurity tunnel. Ransomware claims rose from the second quarter of 2020 through the first quarter of 2021, but claims dropped by 50% in the second quarter of 2021, a trend that continued through the third quarter of the year. In roughly the same time frame, ransomware claims resulting in a ransom payment shrank from 44% in the third quarter of 2020 to just 12% in Q3 2021.[12]

Forward-thinking organizations are spending money to build holistic, robust cybersecurity programs that protect healthcare information and the operational visit. They're implementing information security programs that provide the visibility required so their people can properly identify, detect, respond to and contain any threats.

[11] Source: https://www.healthlawyersblog.com/healthcare-providers-face-ransomware-risks
[12] Source: https://www.csoonline.com/article/3638108/decline-in-ransomware-claims-could-spark-change-for-cyber-insurance.html

The future may be uncertain, but there is one prediction: from a cyber insurance standpoint, especially in healthcare, the threat landscape is rapidly evolving and more changes are coming. The cyber insurance space is also undergoing rapid changes, and your cybersecurity efforts must keep pace.

Organizations must be proactive, involved and prepared to maintain adequate cybersecurity insurance coverage. Be aware of renewal deadlines and ensure your security protocols are in line with coverages.

Pause to Consider

1. What security technologies does your organization use to identify, respond to, and contain cyberattacks?
2. Do you have a cyber insurance policy? And, if so, do you understand what it covers and its limitations?
3. How often does your organization review its security requirements?

The Government's Renewed Focus on Cybersecurity

Few could imagine that a ransomware attack on an oil and gas pipeline would have real-world impacts on the healthcare industry. But the Colonial Pipeline attack was both audacious in its scope and long-lasting for motorists along the East Coast who struggled to find gasoline for more than a month while the company slowly recovered.

Federal regulatory agencies have long focused on increasing cybersecurity, but those efforts have ramped up over the previous two years. Shortly after the Colonial Pipeline breach, where the company paid $5 million in digital currency to recover its data,[13] the U.S. Department of Justice announced its intention to give ransomware attacks the same priority as terrorist attacks. Leaders in Washington will receive case details and technical information as investigations proceed. Investigations that require central notification include cases involving: counter anti-virus services, illicit online forums or marketplaces, cryptocurrency exchanges, bulletproof hosting services, botnets and online money laundering services.[14]

Since healthcare data breaches continue to cost the most to mitigate, even bills and regulations that don't directly affect healthcare bear close monitoring. The influx of regulations is similar to what occurred in the financial services industry over data security related to credit and debit cards. Although data breaches seemingly occur daily, healthcare is particularly vulnerable because of the sheer number of connected technology systems, the 24/7/365 nature of healthcare, technology spending that lags other major industries, and the value of healthcare data.

"Since healthcare data breaches continue to cost the most to mitigate, even bills and regulations that don't directly affect healthcare bear close monitoring."

Since January 2021, Congress has introduced more than 300 bills related in some way to cybersecurity.[15] Many will have no bearing on healthcare, but the sheer number shows the increasing importance of this issue and the responsibility of healthcare IT leaders to keep close watch. The 2021 infrastructure bill includes a $1 billion grant fund to encourage state and local government spending on cybersecurity. Only one-third of states include budgetary line items related to cybersecurity spending, and the grant money is designed to encourage greater awareness and adoption of cyber spending among government entities.

Regulators also have been busy over the past 18 months. The Office of Foreign Assets Control (OFAC), part of the U.S. Department of the Treasury, has adopted new guidelines regarding the payment of ransomware — just say no. According to guidance, "license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial."[16]

[13] Source: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
[14] Source: https://cisomag.eccouncil.org/u-s-doj-gives-ransomware-attacks-same-priority-as-terrorist-attacks/
[15] Source: https://www-csoonline-com.cdn.ampproject.org/c/s/www.csoonline.com/article/3639019/whats-next-in-congress-for-cybersecurity-after-enactment-of-the-infrastructure-bill.amp.html
[16] Source: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

In addition to the stick of ransomware payment, the feds also are dangling carrots to encourage self-initiated, timely and complete reporting of ransomware attacks that could potentially mitigate future enforcement actions. The OAFC is paying close attention because many ransomware attacks originate from foreign actors who may want to undermine national security and foreign policy objectives. The Treasury Department is also cracking down on using digital currencies in financial crimes — including ransomware. The department blocked trades between U.S. entities and a Russian cryptocurrency exchange that the government says derives 40% of its trading volume from illegal activities.

The cost of cybersecurity is on the rise for everyone, partly due to a new Department of Homeland Security (DHS) cybersecurity technician recruitment effort that will raise the upper limit for employee pay to as high as $332,100 in certain circumstances. Salaries for cybersecurity personnel have skyrocketed as staffing needs empty the pool of qualified workers, an issue that shows no signs of lessening. The federal government paying big salaries is sure to put pressure on private industry to keep pace. The department is looking to fill multiple roles, including cyber response, risk and strategic analysis, vulnerability detection and assessment, intelligence and investigation, networks and systems engineering, digital forensics and forensics analysis and software assurance.[17]

Healthcare organizations cannot afford to sit on the sidelines and wait for new government and/or industry mandates on cybersecurity protections. Breaches are prohibitively expensive to remediate in terms of real dollars, the loss of business and the loss of standing against competitors. Additional government scrutiny is likely to bring new and increased penalties. And while government funding may help, its impact will be negligible compared with the cost required to adopt a robust cybersecurity strategy.

"Salaries for cybersecurity personnel have skyrocketed as staffing needs empty the pool of qualified workers, an issue that shows no signs of lessening."

Those strategies should be based on a regulatory standard such as those from the National Institute of Standards and Technology (NIST), which will better position you to respond to any regulatory changes.

Pause to Consider

1. How does your organization keep up with regulations affecting cybersecurity?
2. How does your cybersecurity spend compare to leading industries?
3. When was the last time you looked at IT security salaries or considered outsourcing IT security functions?

[17] Source: https://www.zdnet.com/article/the-us-government-just-launched-a-big-push-to-fill-cybersecurity-jobs-with-salaries-to-match/

Can You Afford Good Cybersecurity?

Ransomware attacks across industries have increased 300% since 2020, and security experts predict these attacks will threaten companies for years to come.[18] Healthcare organizations remain the number one target for ransomware attacks.

Unfortunately, many healthcare organizations have limited or zero visibility into their cybersecurity environment. They don't have basic monitoring, system visibility or log management and might not recognize they're under attack for months. Likewise, if an incident is detected, their ability to thoroughly investigate and understand the problem — much less mitigate it — is extremely limited. What they don't know could definitely harm them and their patients.

Stated in an earnings report, a San Diego-based health system reportedly incurred $112.7 million in lost revenue and added expenses from a 2021 cyberattack. It is estimated that it lost $91.6 million in revenue and incurred $21.1 million in added expenses related to ransomware attack recovery. In addition to direct costs and lost revenue, the health system faces possible class-action lawsuits from patients affected in the attack. [19] They are among the health systems that have been upfront about attacks, spelling a new openness that sheds light on this critical issue.

Understandably, hospitals are worried first and foremost about patient safety in a cybersecurity attack. Many facilities will pay the ransom to ensure patient care is minimally disrupted, because no care provider wants bad outcomes to occur as a result of a ransomware incident.

Even if patients are not at immediate risk, an attack can cause longer-term care disruption. An organization might need to delay scheduling for preventative care, routine tests and screenings. Reputational damage to an organization can indirectly disrupt patient care longer than the attack itself as patients avoid the provider.

"Reputational damage to an organization can indirectly disrupt patient care longer than the attack itself as patients avoid the provider."

In the above attack, the health system was forced to stop using its EHR software for nearly a month. This meant processing patient information offline, slower data processing and delayed care. In other ransomware attacks, hospitals resort to pen-and-paper operations until an attack is resolved, which can severely limit patient throughput. Also, some caregivers are not accustomed to manual workflows and can struggle with delivery.

[18] Source: https://www.beckershospitalreview.com/cybersecurity/ransomware-attacks-will-be-daily-for-5-years-nsa-chief-says.html
[19] Source: https://www.beckershospitalreview.com/finance/scripps-records-q3-operating-loss-notes-cyberattack-cost-of-112-7m.html

In addition, if federal agencies determine that an attack occurred because an organization was out of compliance with HIPAA, regulatory costs — including fines — and remediation expenses can add up fast, not to mention the prospect of patient litigation.

Security is comprised of confidentiality, integrity and availability (CIA). In healthcare, confidentiality is important, but availability is the most vital leg of the triad. Given today's interconnected healthcare environment and healthcare practitioner reliance on data to deliver care, IT systems must be online and working at all times. While nobody wants their data exposed on the dark web, system availability could mean the difference between life or death.

The disruption of healthcare systems and data due to a cyber incident creates serious impacts to patients and the care available in their communities. When building an effective cybersecurity program, availability must be prioritized while downtime must be minimized.

"The disruption of healthcare systems and data due to a cyber incident creates serious impacts to patients and the care available in their communities."

Protecting healthcare technology infrastructure can be expensive, although probably less costly than a successful ransomware attack. The average cost to resolve a ransomware attack, including downtime, labor, device cost, network cost, lost opportunity and ransom paid, is an estimated $9.23 million, a 30% increase over 2020.[20] In addition, hospitals and other entities that pay ransomware extortion demands might be subject to civil monetary penalties.[21]

To provide 24/7 systems availability, an organization must employ a minimum of eight to twelve people, each with an estimated average IT salary of $75,000 per year or more, plus benefits. Around-the-clock coverage is important not only because of the number of alerts coming in, but also because attacks can originate from anywhere in the world. Bad actors never sleep, so monitoring and threat hunting in networks must function on the same schedule.

Even before an organization purchases new security tech, annual labor costs can be close to $1 million. This is more than most health systems can pay without breaking budgets, but doing nothing is not an option. More healthcare organizations are realizing that it makes financial sense to outsource their security operations center (SOC) to ensure 24/7 availability.

[20] Source: https://www.ibm.com/security/data-breach?mhsrc=ibmsearch_a&mhq=cost%20of%20a%20data%20breach
[21] Source: https://racmonitor.com/federal-authorities-may-impose-civil-penalties-against-hospitals-paying-ransomware-demands/

Finding, training and retaining qualified people can be difficult. Qualified information security professionals are scarce and in demand. In a metropolitan area, it's probably not as difficult to hire, but healthcare entities can find themselves competing for that talent with other industries. Managed security service providers (MSSPs) take on the expenses of recruiting, hiring and training analysts, then spread these resources across multiple clients. Healthcare organizations buy the service and don't have to worry about adding staff to their own payrolls or retaining sought-after security professionals.

Rampant ransomware and the potential disruption to patient care are driving healthcare organizations to raise the bar of cybersecurity. Developing, maintaining and testing a disaster recovery plan that includes backups can help organizations recover from attacks, natural disasters and other adverse events.

Eventually, there will be fewer vulnerable cybercrime targets, but this won't happen overnight. Unfortunately, many healthcare entities will learn the hard way that their cybersecurity profile wasn't "good enough" after all.

Pause to Consider

1. Do you have a current disaster recovery plan, and how often do you test it?
2. If your organization is attacked, what measures do you have in place to minimize patient care disruption?
3. What steps is your organization taking to guard against future ransomware attacks?

Mitigating Risk Through Identity and Access Management

Trust no one. Authoritarian governments aside, zero trust is the ultimate IT security protocol, demanding that every person be validated and authenticated at each login to each computer system or application.

Zero trust may work in some industries, but it's a bridge too far for most healthcare organizations, especially in patient-facing areas where timely access to data could have life-and-death consequences. Not to mention that admitting privileges and nursing shortages create a revolving door of new users. If a user requires access to billing, claims and electronic medical records to complete a task, for example, that's three requests for authentication and validation. For most organizations, these dynamics have created a user profile and identity and access management (IAM) nightmare.

Now imagine an emergency department physician who needs immediate access to a patient. Most organizations would simply copy a profile of another ED physician to grant access quickly, but this action could give the new physician more access than necessary.

"Three-quarters of breaches can be attributed to unauthorized access traced to granting too much privileged access to third parties."

With similar processes occurring hundreds of times a month, cleaning up granted permissions can overwhelm most IT teams. This reality underscores why IAM has gained prominence and has become a stepping stone toward a zero trust model. Many organizations are strengthening their IAM strategy and processes while also considering other technical means, like microsegmentation, to reduce cybersecurity risk.

While not as restrictive as zero trust, IAM and microsegmentation protocols can help minimize the impact of a cyberattack or breach by limiting the ability for bad actors to move from machine to machine to further infiltrate an IT system. Ring-fencing access through microsegmentation limits regulatory and compliance requirements to these segmented environments.

Three-quarters of breaches can be attributed to unauthorized access traced to granting too much privileged access to third parties, according to a recent survey. Nearly two-thirds of organizations failed to assess or miscalculated third party risks, and more than half failed to assess third party security and privacy practices before granting access.[22]

The massive Target hack several years ago began with entry through an environmental contractor where the attackers were able to cross other systems to access sensitive credit card information. Hospitals and health systems, unfortunately, are prone to these types of attacks because of the sheer volume of required technology connections.

[22] Source: https://www.cpomagazine.com/cyber-security/51-of-organizations-experienced-a-third-party-data-breach-after-overlooking-external-access-privileges/

Hospitals and health systems are complex from an IT technology standpoint. Mainstream technology systems such as EHRs, PACS, labs, pharmacy, supply chain and notification systems share connectivity with hundreds of other systems, from ancillary and legacy systems to medical devices, environmental controls, and much more. The movement of data and services to the cloud only complicates matters, leaving little doubt why healthcare suffers the greatest number of breaches that cost the most to remediate.

Despite the inherent security challenges, a slower rate of adoption of zero trust practices will be the norm in healthcare, with the reality that physicians want access to everything, everywhere and at any time. If it were your spouse, parent or child whose chart or results the physician was reviewing remotely, you'd probably want the physician to have easy and unfettered access to that data, too.

Naturally, physicians want to provide world class healthcare, which could be compromised if a doctor has to pass through a series of checks and balances to get access to a solution, asset or specific portion of the network. A tradeoff exists between absolute zero trust and the needs of healthcare. Without proper management, a zero trust model can loosen, with risk and exposure creeping into an organization without good security hygiene.

Many organizations believe that single sign-on (SSO) is that tradeoff between trust and access. However, SSO is more of a business enabler and employee satisfier than it is a security initiative. Single sign-on actually can mask a poor authentication scheme if it, perhaps, requires a three-character password or doesn't prompt for frequent password changes. Proximity badges or tokens that allow access to devices within a certain radius or within a specific room can be an adequate safeguard without requiring a true zero trust model.

Both multi-factor authentication (MFA) and microsegmentation initiatives represent a middle ground between a wide-open network and the zero trust model. An initial step could be to create a virtual local area network (VLAN) to compartmentalize certain machines or departments. Microsegmentation takes the VLAN model a step further, grouping machines or departments based on pre-determined criteria such as job function or logical patient journeys.

But no segmentation method will work as needed without an organization first understanding where critical data exists in its IT systems and how systems interconnect. While that sounds simple, creating such a report can be time-consuming and expensive. But it's a critical step in developing a robust cybersecurity program. Once you identify where data resides and how it moves between systems, you can begin creating segmentation points around critical data to limit potential damage from a breach or attack.

Another critical consideration is company culture, governance and buy-in throughout the organization. Many employees will resist any workflow alterations, which requires effective change management strategies to overcome. Technology and change management go hand-in-hand to bring lasting improvements in cybersecurity.

Pause to Consider

1. How does your organization monitor ongoing threats to the network?
2. What steps have you taken to isolate/secure areas where sensitive data resides?
3. What risk mitigation strategies are you employing?

Were We Right?

A Look at Fortified's 2021 Predictions

Prediction

Double-Digit Increase in Breaches: Healthcare again will experience a double-digit increase in data breaches, fueled by email phishing and ransomware attacks.

So how did we do?

We didn't hit the mark for 2021, which initially sounds like good news. But before the celebrations begin, breaches rose 6.7% compared to the same period last year and topped 700 for the year — setting another record. Until the industry gets serious about information security, this unfortunate trend will continue.

Prediction

Larger Spend on Cybersecurity: The C-suite will recognize and prioritize high value risks such as larger threat surface areas and the number of endpoints that need protecting. Spending will be on software and services, rather than people.

So how did we do?

We have seen more spend dedicated to cybersecurity, partly because of the number of highly publicized breaches and attacks that have occurred. Healthcare continues to be viewed by threat actors as an easy target with a large payoff. Despite increased spending, healthcare is seen as a laggard in the adoption of resilient, robust and secure IT practices and processes.

Prediction

Focus on Verifying Credentials and Access: Organizations will continue to move toward tighter access security, including multi-factor authentication (MFA), zero trust, identify access management (IAM) and cloud access security brokers (CASB) to better control access to data and systems.

So how did we do?

With breaches steadily increasing, cyber insurance carriers are starting to focus on credential verification via multi-factor authentication (MFA). Furthermore, some carriers are requiring MFA in order to grant coverage. Increased rates and coverage lapses are forcing executives to take a hard look at these protections. We're also seeing wider adoption of segmentation projects and zero trust technologies and architectures to secure information, users and assets.

Prediction

The Advent of Tools Rationalization: IT departments finally begin to embrace tools rationalization, which can identify and eliminate security gaps, reduce expenses and ensure best-in-class software is being deployed.

So how did we do?

We are seeing more companies replace legacy software like traditional anti-virus with advanced endpoint detection and response (EDR) solutions. Some organizations are also evaluating current tools to ensure they are utilizing the platform's complete functionality. However, healthcare organizations should be wary of companies that bundle different security solutions together at too-good-to-be-true prices as your perceived and actual risk reduction may be materially different. This issue will continue to resonate as the four walls of the hospital blur and organizations increase use of public cloud services.

Cybersecurity Outlook 2022

Number, Severity of Breaches Grows

While the number of breaches didn't rise to the double-digit growth we expected in 2021, the trend was higher. And so it will be in 2022, combined, unfortunately, with an increased attack severity. More often, hospitals are shutting down or delaying patient care because of hacking incidents, and the costs to patients continue to rise.

SolarWinds of Healthcare

Most cyberattacks on healthcare are isolated incidents affecting one hospital or health system. A SolarWinds-type healthcare breach is coming, leaving dozens or hundreds of hospitals vulnerable. There have been isolated incidents involving medical transcription and a niche EHR in recent years, but the big one is coming.

Adoption of EDR Solutions Grows

It's time for endpoint detection and response (EDR) solutions to shine. Traditional signature-based antivirus is reactive, catching malware after it's already been delivered (if it's caught at all). An EDR solution should monitor for threats in real-time by analyzing system-level data and behaviors to uncover threat patterns and respond to those threats while providing contextual information to the appropriate personnel and retaining threat data for later analysis.

More Partnering with MSSPs

Will this be the year healthcare organizations finally begin to take IT security seriously? More breaches, more ransomware attacks, regulatory changes and tightening cyber insurance standards will pressure healthcare executives to take definitive action. Higher salaries for IT security workers will price many hospitals out of in-house security, and they will look to managed security services providers for cost-effective assistance.

Moving Forward

Be proactive

It is important to remember that the number of successful breaches reported to OCR is not equal to the number of attacks. Today, all of healthcare has a bullseye on its back and is being attacked thousands of times daily. No longer can healthcare organizations hope to not be targeted and attacked. It's not a question of if, but when. Prevention and mitigation are the only acceptable responses. Hoping for the best was never an acceptable position, and today is even less so.

Be supportive

Government help may be on the way, but it will take a long time to fully implement. Unlike the healthcare digitization initiative that brought us modern day EHRs, which was a point-in-time investment for the government, cybersecurity initiatives are an increasing expense. And with every organization at a different point of their cybersecurity journey, the initial and ongoing investment can be hard to calculate. It will fall on those of us in healthcare to work with Congress but more importantly within our own industry to do what must be done to protect our institutions and patients.

Stay educated

We have now seen very public displays of data about the type of disruptions cyber events are causing the healthcare industry. This openness and sharing are important to develop a community that is more aware and grows stronger in its cybersecurity journey. Seek out groups, like the monthly Fortified Roundtables, that openly discuss shared experiences and challenges the industry is facing.

Remember the basics

Risk assessments are just the beginning in understanding potential risk and vulnerabilities to your environment. And they are a necessary task that should be accomplished annually. Choosing a framework for your organization and consistently working on improvements in your assessment year over year will help drive your cybersecurity program and will steer your investment decisions.

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

Modern Healthcare
Best Places to Work 2021™