2020 Horizon Report

THE STATE OF CYBERSECURITY IN HEALTHCARE

Fortified
HEALTH SECURITY

President’s Message

As predicted, 2019 has been a historic year for the US healthcare cybersecurity industry with the most breaches ever reported in a 12-month period. These breaches occurred in nearly every state and across every type of organization. They included a broad range of attacks, from phishing to ransomware. Cybercriminals continue to place a high value on the healthcare industry and are using more advanced and scalable tools to cause disruption.

The healthcare industry is vulnerable not only because of the sensitive and valuable information it stores, but also due to the “always on” nature of its business and its need for constant data access. Cybercriminals use the simple fear of being locked out of data access to extort high ransoms from healthcare organizations that are under pressure to get their systems back up and running because patient lives are at stake.

> Cybercriminals continue to place a high value on the healthcare industry and are using more advanced and scalable tools to cause disruption.

Compounding the situation is the Internet of Things (IoT) and Bring Your Own Devices (BYOD) connecting to the network allowing new opportunities for malware to enter the healthcare environment.

Technology companies have recognized the need to bolster their cybersecurity defenses and are also joining in to help healthcare organizations strengthen their security posture. 2019 saw an increase in mergers, acquisitions, and investments by these companies to include or expand upon their cybersecurity capabilities.

This year, the Department of Health and Human Services (HHS) proposed modifications to both the Anti-Kickback Statute (AKS) and the Physician Self-Referral Law (often referred to as the “Stark Law”) that recognized the increased threat of cyberattacks due to digitization and connectivity. The proposed Stark Law changes would allow providers to accept technology-related donations essential to reducing the risk of a data breach or cyberattack.

As we enter 2020, disciplined strategies geared toward reducing risk over time are more important than ever before. Every organization needs a strategy that effectively balances people, process, and technology to navigate this difficult landscape.

An organization’s workforce is still its greatest cybersecurity vulnerability. Healthcare organizations must embrace a greater responsibility to help employees navigate cybersecurity best practices, identify possible phishing attacks, and remain vigilant to solve this immense global challenge. In doing so, they will create not just a more engaged and educated workforce, but also a more secure environment.

Although cyberattacks are getting more sophisticated and targeted, executing fundamental security practices remains key to sustaining a strong cybersecurity program. Organizations that remain disciplined and focused reap rewards over the long term. My hope is that the Horizon Report builds awareness about the cybersecurity landscape in healthcare and provides valuable insight for your program. We welcome your feedback and perspective at: horizonreport@fortifiedhealthsecurity.com. Enjoy.

Regards,

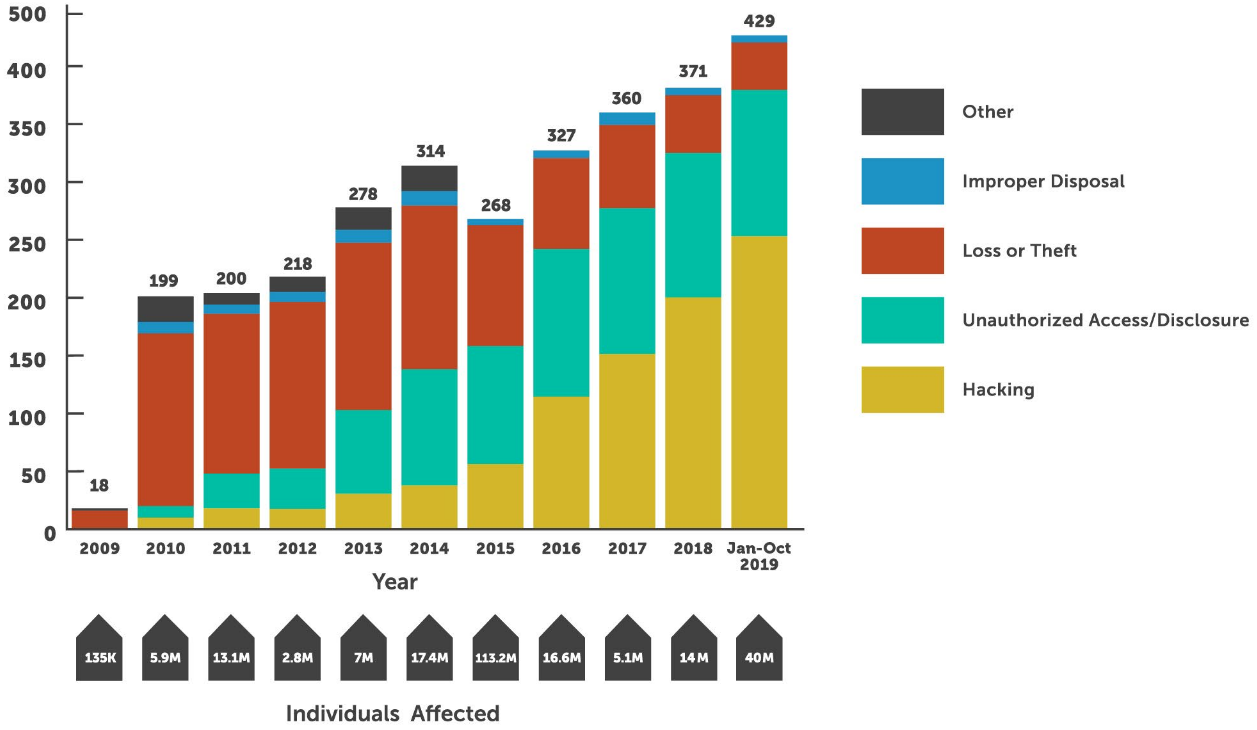
Dan L. Dodson

2019 Year in Review

Previous trends that dominated healthcare cybersecurity continued throughout 2019, and bad actors have accelerated their attacks on healthcare organizations across the country. Ransomware and phishing wreaked havoc, disrupting patient care and costing organizations millions of dollars to remediate and recover critical systems. For the first time ever, more than 400 healthcare organizations reported a breach of 500+ patient records in a single year. Despite continued efforts to make improvements, many still struggle to stay in front of cybercriminals due to limited budgets, human capital challenges, and alert fatigue. It is critical to develop and execute effective cybersecurity programs that are grounded in fundamentals, staffed correctly, and focused on risk mitigation.

This marks the 10th year that the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) collected and posted breach notification information to the public. 2019 also represents the greatest number of reported breaches in a single year. Through the first 10 months, the number of reported breaches increased 38% compared to the same period last year. In total, over 429 entities have reported a major breach so far, which already eclipses the 371 entities impacted in all of 2018. This equates to over 40 million individuals impacted by these reported breaches. We expect the number of entities reporting a breach to surpass 480 by the end of 2019.

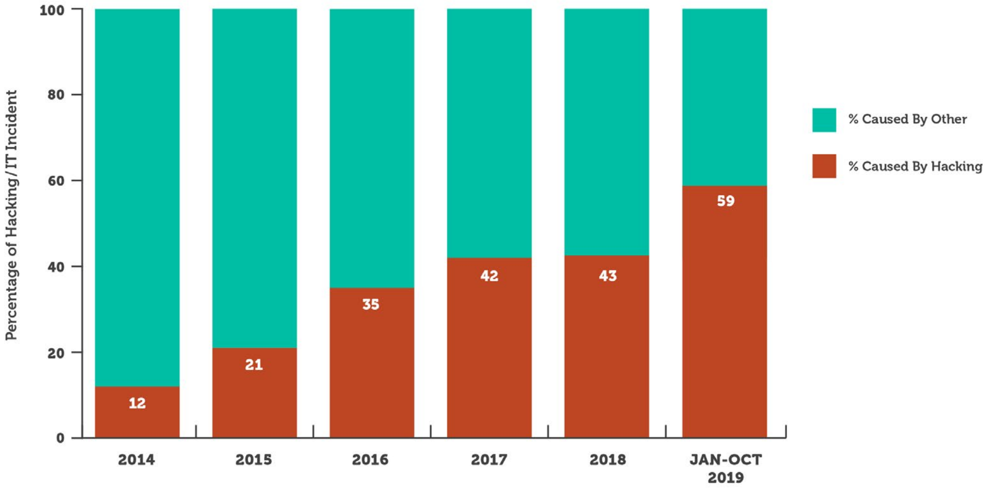
Entities Involved in a Breach [1]



[1] Source: U.S. Department of Health and Human Services Office for Civil Rights

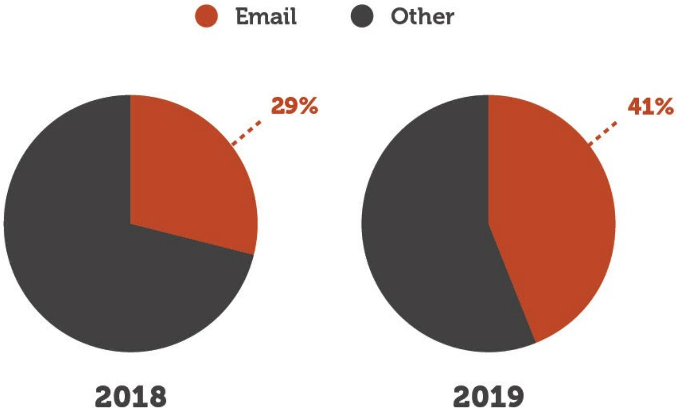
Hacking has been the leading cause of reported breaches since 2016 and this year, for the first time, hacking caused the majority of all reported events at 59%, continuing a steady rise since 2014. This sharp increase is a stark reminder that bad actors remain focused on attacking healthcare and they continue to be successful.

Breaches Caused by Hacking [1]



According to reported breach data, the attack vector most often used by cybercriminals in healthcare this year was email. This highlights the importance of good cyber hygiene within your organization. Investing in user cybersecurity training and implementing an action-driven simulated phishing program have become critically important. Since 2014, the percentage of breaches involving email has increased to over 40%. This represents a significant jump since 2014, and this trend is not likely to slow down. Employees will remain one of your greatest cybersecurity risks.

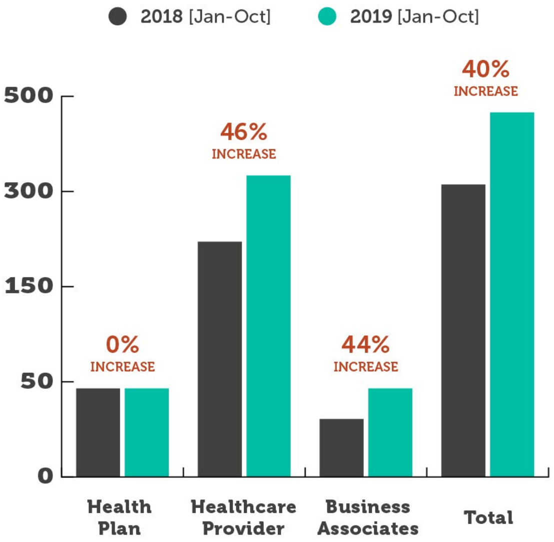
Percent of Breaches via Email [1]



[1] Source: U.S. Department of Health and Human Services Office for Civil Rights

Provider organizations continue to be the most targeted and successfully breached segment of healthcare. Thus far in 2019, more than 334 provider entities have reported a breach and over 22.7 million patients have been impacted. This represents over 78% of all breaches. All three segments: health plan, business associates, and providers, will likely experience a year-over-year increase in reported breaches by the end of 2019.

Entities Involved in a Breach [1]



It is imperative that healthcare organizations build a multi-pronged cybersecurity program that is anchored in risk mitigation. Many organizations suffer from project distractions and culture issues that prevent proper execution of security fundamentals. These challenges are often further exacerbated by the difficulty of attracting the right cybersecurity talent. Make sure your organization remains focused on identifying and reducing risk over time. Given the climate and intensity of attacks, prioritizing a focused and disciplined security culture may prove to be your best defense.

PAUSE TO CONSIDER

1. Is your organization's security program centered on risk mitigation?
2. Are you prepared for a security incident?
3. How are you managing your security culture?

[1] Source: U.S. Department of Health and Human Services Office for Civil Rights

Office for Civil Rights

OCR – Investigation & Fines

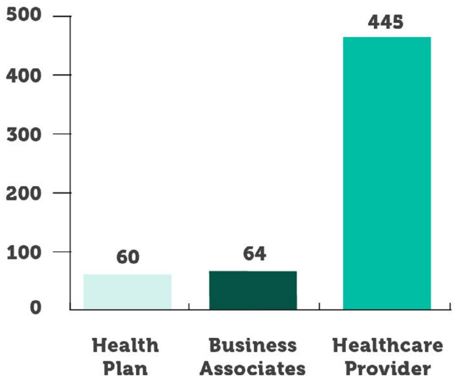
In the first 10 months of 2019, there were eight resolution agreements reached between OCR and healthcare organizations. Each agreement included a steep fine, averaging more than $1.6 million, as well as a multi-year corrective action plan that requires the organization to make improvements to its cybersecurity program.

According to HHS:

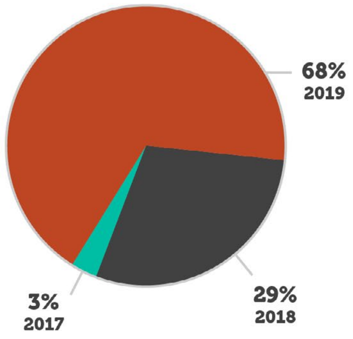
> “A resolution agreement is a settlement agreement signed by HHS and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered 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 571 organizations under investigation for incidents dating back to 2017.

Entities Under Investigation Oct 2019 [1]



Date of Reported Breach [1]



The impact of a breach at any healthcare organization extends well beyond the time it takes to regain full functionality of critical systems. These OCR investigations take a toll on the organization and prove to be a constant reminder of past incidents years after the breach is identified. Conducting an annual risk assessment and, more importantly, making progress against any corrective action plans are critical steps to simplifying the investigation process and potentially limiting fines. Healthcare organizations that take a disciplined, documented, risk-based approach to cybersecurity are more likely to avoid this process altogether. But, should they find themselves working with OCR, they will be in a much better place.

PAUSE TO CONSIDER

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

[1] Source: U.S. Department of Health and Human Services Office for Civil Rights

2019 Market Dynamics

Healthcare organizations faced three significant market forces in 2019, and their impacts will likely last for years to come.

1

CYBERSECURITY TECHNOLOGY CONSOLIDATION

2019 has been a significant year for mergers and acquisitions in cybersecurity, as large companies sought to create more sophisticated platforms, and smaller businesses continued consolidation.

2

RANSOMWARE: STILL WREAKING HAVOC

Ransomware is becoming a more commonly used tool in cyber crimes and can be carried out from anywhere in the world. Major healthcare systems were paralyzed this year by ransomware attacks.

3

STARK LAW REFORM

HHS proposed changes to the Stark Law will allow providers to accept technology-related donations in an effort to reduce cybersecurity risk.

Cybersecurity Technology Consolidation

Mergers and acquisitions have always been a driving force throughout global technology sectors for a myriad of reasons. The continually evolving innovation landscape allows tech companies of every size, scope, and focus to align their resources with other innovative organizations in hopes of better leveraging synergies, driving corporate growth, and ultimately commanding a more significant share of the consumer market. As a result, technology companies continuously evaluate opportunities to strengthen their current product offerings, expand their technology stack into new areas, and in some instances, enter into entirely new market verticals. The cybersecurity technology market was influenced by these forces in 2019 with numerous investments and vendor consolidations.

In recent years, the alarming rise in worldwide cyberattacks and data breaches has prompted a noticeable upswing in cybersecurity mergers and acquisitions within the tech sector. The cybercriminal terrain across virtually every industry is both complex and ever-changing, making companies that specialize in cybersecurity highly desirable assets for technology-centric enterprises. Over the last year alone there have been several significant and strategic moves within the cybersecurity market.

First, the endpoint sector transformed through numerous mergers, investments and initial public offerings (IPOs). A couple of notable mergers include Blackberry's acquisition of Cylance and VMware's acquisition of Carbon Black. Thoma Bravo, a private-equity firm with stakes in several network security companies, has revealed plans to purchase Sophos[2]. Additionally, Crowdstrike raised capital during its summer IPO. These consolidations and capital raises were designed to unlock additional value to clients and strengthen their products.

> The cybercriminal terrain across virtually every industry is both complex and ever-changing, making companies that specialize in cybersecurity highly desirable assets for technology-centric enterprises.

Secondly, there is significant focus around securing the IoT, which includes non-traditional technologies. Medical devices continue to be one of the most vulnerable assets within a healthcare organization and are included in the larger IoT security market. There have been considerable advancements in machine learning, artificial intelligence, and behavioral analytics to assist in solving IoT security challenges and secure medical devices for many organizations. Of course, with advancement comes consolidation and investment. In 2019, there were many Silicon Valley-based companies that raised capital to advance their IoT technology and ramp up sales efforts. As for consolidation, Palo Alto, an organization known for its propensity to purchase leading startups, announced its intent to buy Zingbox[3], an IoT security innovator. Furthermore, device visibility developer ForeScout Technologies acquired SecurityMatters[4], a company that specializes in network protection, variance identification, and device detection and monitoring solutions. Increased consolidation in the IoT cybersecurity market is expected over the next couple of years.

Though there are distinct nuances to each deal, these mergers and investments collectively highlight the growing trend of larger companies using acquisitions to bolster their security offerings through product integration and enhancements, as well as to grow their client portfolios. However, big tech companies aren't the only ones that benefit from aligning their resources and established enterprises with smaller security firms.

[2] Source: https://www.inforisktoday.com/thoma-bravo-to-buy-sophos-for-39-billion-a-13239

[3] Source: https://techcrunch.com/2019/09/04/palo-alto-networks-intends-to-acquire-zingbox-for-75m/

[4] Source: https://www.zdnet.com/article/forescout-technologies-snaps-up-securitymatters-in-113-million-deal/

By expanding their existing suite of competencies to include cybersecurity solutions, technology organizations can do more than command additional market share. These companies are also uniquely equipped to better serve their customers, particularly those in the healthcare space. More importantly, this trend of acquisition is likely to continue for the foreseeable future, prompting CISOs and IT managers across the country to take a closer look at the advantages of working with a technology partner that provides services and solutions across several innovation niches, including network security.

> It is important to meet with your technology partners following the transaction to understand what their technology roadmap looks like. Remember that in some instances, the new owner may need time to finalize the roadmap.

The first thing many healthcare organizations think about in the current climate of mergers, acquisitions, and IPOs is “How will these changes impact my organization?” For the most part, there is little to no immediate impact following a merger, acquisition, or IPO. The real question is how the product will evolve or innovate over time. It is important to meet with your technology partners following the transaction to understand what their technology roadmap looks like. Remember that in some instances, the new owner may need time to finalize the roadmap. The best course of action is to ask questions with an understanding that it may take time to get the real answer. Additionally, it may be the ideal time to assess your existing technology infrastructure and current cybersecurity practices to ensure all internal programs focus on three mission-critical components: people, process, and technology.

Partnering with a managed services organization can immediately simplify the decision-making process. Rather than taking the time to vet individual technology companies for each required element of your security program, healthcare organizations can benefit from engaging a managed services partner to evaluate, select, implement, and manage the right technology. With the technology vendor landscape evolving, this expertise may be more important than ever before.

PAUSE TO CONSIDER

1. **Has your organization been impacted by technology vendor consolidation?**
2. **Do you understand the roadmap of your main technology providers?**
3. **Are you extracting the full value of the technology you already own?**

Ransomware: Still Wreaking Havoc

Ransomware has long proven a major threat to healthcare organizations across the U.S. Marked by the release of malware that locks a digital environment, a ransomware attack prevents users from fully accessing their systems. Once the malware is released, users are urged to pay a designated ransom to regain access to their systems and data in a timely manner. Without adequate back-ups, many health systems find themselves out of service following a severe ransomware attack, which can materially impact patient care.

> Without adequate back-ups, many health systems find themselves out of service following a severe ransomware attack, which can materially impact patient care.

Recent years have seen a steady rise in the total number of malware events in healthcare. The rampant surge of ransomware attacks has prompted cybersecurity and data breach professionals to leverage sophisticated innovations to prevent an outbreak. Unfortunately, despite these efforts, ransomware security breaches continue at a breakneck pace across the healthcare landscape. In September 2019[5] alone, a total of 30 medical enterprises, including hospitals, insurers, and private practices experienced data breaches—many of which were launched by malware resulting in a ransomware outbreak.

> For healthcare organizations it's not just about protecting a patient's private and sensitive information; they also must have instant, continuous access to a patient's records to effectively provide care.

While malware has undoubtedly had an impact across multiple industries, healthcare continues to remain a popular hacker target for one primary reason: cybercriminals recognize hospitals and health systems typically cannot survive without a functioning environment. For healthcare organizations it's not just about protecting a patient's private and sensitive information; they also must have instant, continuous access to a patient's records to effectively provide care.

Without access to critical therapy and treatment data, an entire healthcare organization can quickly find its operations disrupted or even halted entirely. In October 2019, a hospital system in Alabama[6] found its connected platforms debilitated by a successful ransomware onslaught that forced practitioners to turn patients away at three of its locations, treating only the most critical cases during this period of operational upheaval.

As a result of the breach, the health system had to shift to a manual operations mode. Practitioners resorted to tracking care information and patient data using paper copies. Unable to rely on its systems, the organization eventually acceded to cybercriminal demands and paid a ransom to restore its digital platforms. While hospital officials didn't disclose the ransom amount paid, facility executives acknowledged that the organization did purchase a decryption key from cyber attackers to accelerate system restoration and gain full access to sensitive patient information. In addition to the impact on patient care, this event made national news, negatively impacting the reputation of the organization. In all, the cost of the attack is likely measured in the millions.

[5] Source: https://www.beckershospitalreview.com/cybersecurity/why-ransomware-other-cyberattacks-have-been-on-the-rise-inside-hospitals-and-how-to-prevent-them

[6] Source: https://www.healthcareitnews.com/news/alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack

U.S. GOVERNMENT SLIGHTLY SHIFTS STANCE ON PAYING RANSOMS

The recent wave of ransomware attacks has even influenced how the U.S. government handles this type of data breach. For years, the FBI advocated that healthcare executives maintain a zero-tolerance policy for paying hackers to restore their online files, folders, and systems. As ransomware and other malware attacks continue to gain momentum and impact, the federal government is reevaluating its viewpoint.

Make no mistake: the FBI still recommends organizations in any industry never pay the ransom demand. The government asserts that paying a ransom after email phishing or some other type of malware attack will only encourage future hackers to perpetrate similar actions online. Worse yet, even after paying the ransom, a company may still not regain access to its digital ecosystems.

However...

The FBI recently published an updated version of the protocol[7] for companies navigating a malware event. In the newly posted document, the FBI does recognize that much like the health system in Alabama, when businesses cannot properly function after a cybersecurity lapse, executives should carefully consider all options to safeguard their systems as well as their staff and consumers.

> The government asserts that paying a ransom after email phishing or some other type of malware attack will only encourage future hackers to perpetrate similar actions online.

The recent policy changes add an additional layer to the already exceptionally gray and uncertain landscape of cybersecurity. What isn't uncertain? Ransomware, at least in the near future, isn't going anywhere and will likely continue to target healthcare organizations using a myriad of channels. Malware is no longer transferred just through email; it is seen on mobile devices and social media because they are being allowed on enterprise networks. As a result, healthcare organizations must always remain vigilant about their cybersecurity practices to keep their platforms well-protected.

PAUSE TO CONSIDER

1. **Is your organization prepared for a potential ransomware attack?**
2. **Have you adequately tested your back-ups?**
3. **Does the entire leadership team understand the potential impact of a ransomware attack?**

[7] Source: https://www.ic3.gov/media/2019/191002.aspx

Stark Law Reform

HHS recently released proposed modifications designed to significantly update and modernize both the Anti-Kickback Statute (AKS) and the Physician Self-Referral Law (commonly known as "Stark Law"). First enacted in 1989, the Stark Law refers to a set of U.S. federal laws that expressly prohibit the practice of physician self-referral for financial gain. More specifically, it explicitly prevents practitioners from referring Medicare or Medicaid patients to designated health services (DHS) that have an existing financial relationship with the referring physician or the referring physician's family members.

STARK LAW INITIALLY ENACTED BASED ON FEE-FOR-SERVICE CARE PRACTICES

Though mostly untouched over the last four decades, the Stark Law is now gaining substantial attention from clinicians, patients, and U.S. government officials due to the country's evolving healthcare system. In 1989, U.S. healthcare was primarily charged on a fee-for-service basis. As a result, the federal government recognized that self-interest and financial gain might influence a physician's referral decision.

While there have always been statutory and regulatory exceptions, today the Stark Law ultimately mandates that in order to prevent profit motive taking precedence over patient care, physicians are not permitted to make referrals for Medicaid patients to a medical entity with which they have an existing financial relationship. Additionally, the Stark Law prohibits a conflicting entity from filing payment claims with Medicare for services rendered that violate the Stark Law. In fact, the U.S. government stipulates that Medicare cannot legally pay requests submitted from these practices.

PROPOSED UPDATES TO STARK LAW WILL CONSIDER VALUE-BASED CARE

The legislators who devised the fraud rules of the Stark Law did so to safeguard patients navigating a fee-for-service healthcare system. However, policymakers have realized that the existing protocol of the Stark Law does not always align with value-based care practices that strive to promote quality, not necessarily volume, throughout the treatment process.

> The proposed rules support the value-based care initiative by eliminating existing legal barriers that may currently hinder providers from working collaboratively in the best interest of patients, specifically concerning digital environments and collective network security efforts.

The new safe harbor proposal recognizes that the digitization and connectivity of the U.S. healthcare delivery system required for interoperability and collaboration within a value-based care program also elevates the threat of cyberattacks across the entire healthcare landscape. As practices increase data sharing across multiple systems and sources, a single compromised environment could cause a data breach that shuts down an entire digital ecosystem. As a result of interoperability, a well-orchestrated attack could materially impact the delivery of care within a community.

The proposed Stark Law changes would allow providers to accept technology-related donations that are essential to reducing the risk of a data breach or cyberattack. However, the current proposal outlines limits on what can be donated. For example, hardware is not considered a compliant donation, but the rule does allow network security training services, software, business continuity and data recovery services, practices associated with security risk assessments, threat-sharing services, and cybersecurity-as-a-service offerings.

STARK LAW CYBERSECURITY LEGISLATION COULD DECREASE COST BURDEN FOR PATIENTS

The proposed updates for physician self-referral laws are currently under review. The proposal is open for comments from impacted providers until December 31, 2019. After commentary has closed, Congress will review the input to determine if anything in the changes warrants a modification. From there, they will vote to decide if these new rules will become permanent legislation.

By expanding opportunities for a safe digital environment, the new Stark Law proposals may also directly impact patient payments.

Cyberattacks cost the average healthcare organization approximately $1.4 million in recovery fees and lost productivity.[8]

Additionally, administrative costs and data loss prevention initiatives cost the U.S. healthcare system hundreds of billions of dollars annually. Allowing providers to receive donated cybersecurity resources can prove a critical step toward lowering the cost burden for patients across every phase of the care continuum. As health systems evaluate third-party risk these potential changes to the Stark Law could materially impact your strategy.

PAUSE TO CONSIDER

1. **How would these potential changes impact your organization?**
2. **Are your colleagues in provider relations adhering to these changes?**
3. **What impact would these changes have on your business associate agreements (BAAs) or third-party risk management program?**

[8] Source: https://healthitsecurity.com/news/healthcare-cyberattacks-cost-1.4-million-on-average-in-recovery

Were We Right?
A Look at Fortified's 2019 Predictions

PREDICTION

Single-Digit Increase in Breaches: Healthcare will experience a 5-9% increase in the number of entities breached over 2018, with providers being the most targeted and exploited segment.

So how did we do?

Through the first 10 months of 2019, the number of breaches reported by OCR[1] increased 16% over the full year 2018. Fortified expects the full year increase to be over 20%. For the 10th consecutive year, providers remain the most targeted and breached segment in healthcare.

PREDICTION

Increased Investment in Connected Medical Device & IOT Security: Health systems will invest more heavily in medical device security by leveraging new technologies and strengthening governance programs between IT, security, and clinical engineering.

So how did we do?

With the advancement in technology options, many healthcare organizations began the selection process to procure medical device and IoT security technology in 2019. The primary use case was to gain better visibility into medical device security issues by first identifying all the assets on the network and then monitoring their behavior over time. Many organizations made decisions on which technology to procure, and many organizations find themselves in the middle of proof-of-concept development. Most are still determining how to appropriately operationalize these technologies to extract the maximum value.

PREDICTION

Increased Threat from Cryptomining: Cybercriminals are exploiting known vulnerabilities to steal the processing power of these devices to mine for cryptocurrencies. Cryptomining continues to rise as cybercriminals are not content with only stealing data like they once were. We expect this threat to increase in 2019.

So how did we do?

Cryptojacking is the process of stealing computing resources to generate cryptocurrency (i.e., cryptomining). According to the 2019 SonicWall Cyber Threat Report mid-year update[9], the volume of cryptojacking hit 52.7 million registered attacks in the first six months of 2019, with over 33 million of those resulting from Coinhive use. This is a 9% overall increase from the last six months of 2018. The larger trend is difficult to assess in part due to the extreme volatility of cryptocurrency prices during 2019 and the shuttering of Coinhive in March, which was widely used by malware groups to cryptojack computing resources. Organizations need to continue to monitor resource utilization on critical assets where this type of malware may bring on an availability impact, as new players and additional cryptocurrencies are introduced.

PREDICTION

Continued Targeted Phishing Attacks: Today it is estimated that 90% of all malware is delivered via email to end users. Targeted and sophisticated phishing campaigns, commonly known as spearphishing, make bad actors more effective and will likely intensify as hackers look to achieve a higher level of success.

So how did we do?

According to the reported OCR breach data[1], 41% of successful attacks involved email. This is up from 33% in 2018, representing the sixth consecutive year of increases. Individuals who have access to email on your network remain one of your biggest threats. Organizations should continue to invest in security awareness training and conduct regular simulated phishing exercises.

[1] Source: U.S. Department of Health and Human Services Office for Civil Rights

[9] Source: https://www.sonicwall.com/resources/white-papers/mid-year-update-2019-sonicwall-cyber-threat-report/

Looking Ahead

CYBERSECURITY OUTLOOK 2020

1

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.

2

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.

3

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.

4

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.

Moving Forward

PRACTICE SIMULATED PHISHING

As our adversaries continue to utilize email as their weapon of choice, it is critical that every healthcare organization develop and implement a simulated phishing program. Be sure to consider culture and human resource requirements to make this program most effective.

UNDERSTAND THIRD-PARTY RISK

It is difficult for some organizations to effectively manage third-party risk due to technology sprawl and the ever-expanding vendor network; however, establishing strong governance and a risk-based model is imperative to protect your organization.

OPERATIONALIZE YOUR TECHNOLOGY

Healthcare organizations often look to technology alone to solve their cybersecurity problems. As a result, they purchase technical point solutions without adequately planning for the ongoing management of these tools, leading to the misconception that their organization is more protected than it actually is. Don’t forget the real value of these tools lies in how you manage and monitor them over time.

CREATE A COMMUNITY

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.

CONTACT US TO START ON THE PATH FROM COMPLIANCE TO CONFIDENCE®.

For more information, visit our website at:

fortifiedhealthsecurity.com

INQUIRIES

1 (615) 600-4002

horizonreport@fortifiedhealthsecurity.com

OFFICE

2550 Meridian Blvd, Suite 190
Franklin, TN 37067

FOLLOW US

ABOUT FORTIFIED HEALTH SECURITY

Fortified Health Security is a leader in cybersecurity, compliance, and managed services dedicated to helping healthcare organizations overcome operational and regulatory challenges. Founded in 2009, Fortified has established a heritage of excellence, compliance, and innovation. Today, Fortified works closely with organizations across the healthcare continuum to assess risks, implement safeguards to protect sensitive information, and assist with compliance with state, HIPAA and other federal regulations. Fortified was named the 2018 North American Health IoT Company of the Year by Frost & Sullivan and a Top Provider of Medical Device & IoT Cybersecurity Solutions by Black Book for its impressive portfolio of healthcare cybersecurity solutions.

ABOUT THE AUTHORS

Dan L. Dodson serves as President of Fortified Health Security where he helps healthcare organizations effectively develop the best path forward for their security program based on their unique situation. Prior to joining Fortified, Dan served as Executive Vice President for Santa Rosa Consulting, a healthcare-focused IT consulting firm, where he led various business units as well as the sales 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. A thought leader in the healthcare cybersecurity space, Dan has been featured in Becker's Hospital Review, Healthcare Business Today, Healthcare Innovation News, and other media outlets. In 2018, Dan was recognized as a rising healthcare leader under 40 by Becker's Hospital Review. He has also spoken at industry-leading events and conferences, including HIT Summits, CHIME and HIMSS events. He currently serves on the Southern Methodist University Cyber Advisory Board. Dan holds 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). William retired after serving 20+ years in 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).