2019 MID-YEAR
Horizon Report

THE STATE OF CYBERSECURITY IN HEALTHCARE

Fortified
HEALTH SECURITY

President's Message

The U.S. healthcare market continues to face an increase in cybersecurity threats from bad actors, and it looks as if 2019 will top last year for the most breaches ever reported. With momentum on the side of our adversaries, it is important that we, as healthcare cybersecurity leaders, continue to focus on and execute security fundamentals. Oftentimes internal cybersecurity teams become sidetracked by other IT projects, and the daily requirements of a solid cybersecurity program get pushed to the side. This dynamic is playing out across the country, and coupled with a weak security training program, many organizations find themselves vulnerable. It is critical to remember the fundamentals when evaluating your cybersecurity program.

With momentum on the side of our adversaries, it is important that we, as healthcare cybersecurity leaders, continue to focus on and execute security fundamentals.

On top of the increased pressures from bad actors and a dynamically changing threat landscape, there are three market realities that continue to provide challenges to most healthcare organizations. First, there is enormous demand for cybersecurity talent. This is a worldwide issue that impacts all verticals and requires healthcare organizations to be thoughtful about how they attract, train, and retain cybersecurity talent. Without the right level of commitment and focus, the cybersecurity team will become a revolving door at all levels. Secondly, there continue to be advancements in cybersecurity technology that require specific expertise to properly operationalize and extract the full protection and value of each tool. When implementing new security technology, make sure you properly plan for the right level of resources to protect your organization. Technology that is not monitored or managed will fall behind quickly. Lastly, it continues to be difficult to gain C-suite buy-in for security initiatives across the entire healthcare organization. As investments in cybersecurity increase, it is critical that security and IT leaders demonstrate the value of each dollar spent so our colleagues can easily understand how security is, at its heart, a patient safety issue. Demonstrating how your cybersecurity program has strengthened over time, based on investments made, is critical for ongoing, system-wide support.

As investments in cybersecurity increase, it is critical that security and IT leaders demonstrate the value of each dollar spent so our colleagues can easily understand how security is, at its heart, a patient safety issue.

I see many of these challenges playing out in healthcare organizations of all sizes and financial strength. More money spent on security doesn't necessarily mean more sophistication or a more mature security program. Know that you are not alone, and I strongly advocate for security professionals to communicate, network, and collaborate to help strengthen the cybersecurity posture of healthcare.

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,

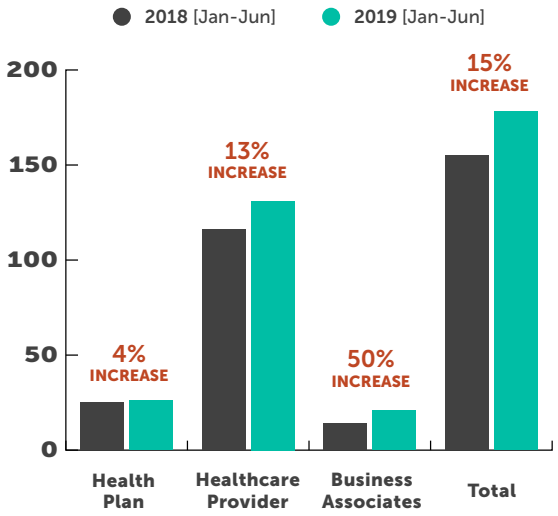
Dan L. Dodson

2019 Mid-Year in Review

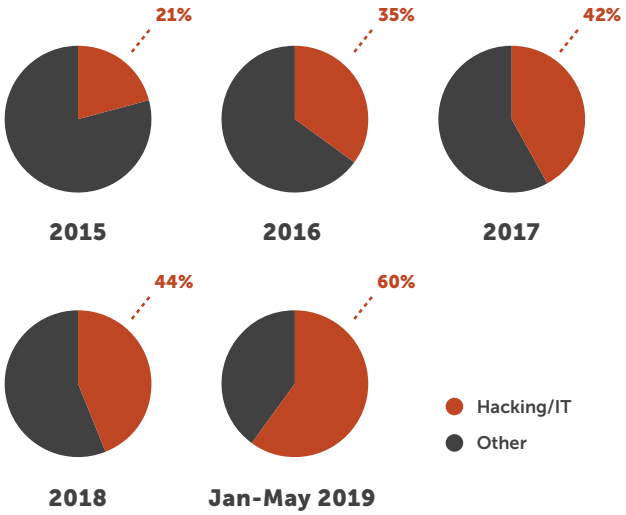
The healthcare industry continues to top the charts as the most widely attacked vertical and again led all industries with the highest number of cybersecurity breaches in 2018[1]. This trend has accelerated in 2019, with the number of reported breaches through May increasing by 15% over the same period last year. This represents an increase of 23 entities impacted according to breaches reported to the U.S. Department of Health and Human Services Office for Civil Rights (OCR).

On top of the healthcare industry overall seeing an increasing number of breaches, every segment of the healthcare industry has experienced more breaches thus far in 2019 compared to the same period in 2018. Healthcare providers continued to be the most targeted and, as in previous years, have experienced the most breaches with 74% of all incidences. Business associates faced a 50% increase in the number of breaches year-over-year, representing the largest increase of any healthcare segment. Health plans faced the smallest increase at 4% year-over-year.

Entities Involved in a Breach [2]



Percent of Breaches via Hacking/IT Incidents [2]



Hacking continues to be the leading cause of reported breaches to date in 2019 with more than 60% of incidences occurring because of hacking.

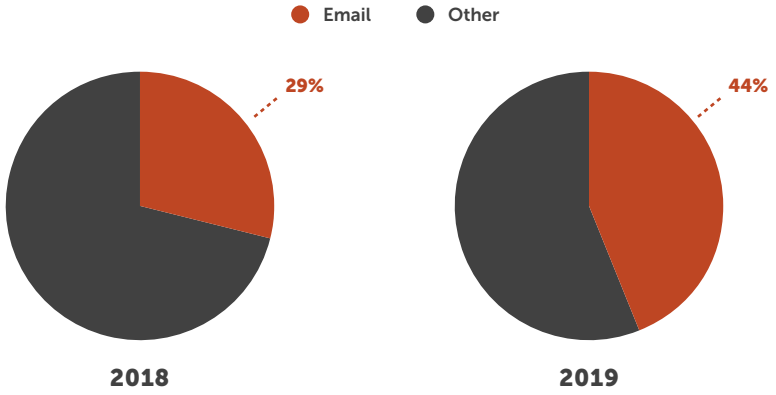
These successful attacks have impacted almost four million patients thus far in 2019. This represents a significant increase over prior years as 44% of all reported breaches in 2018 were caused by hacking. The percentage of reported breaches caused by hacking has increased every year since 2012 and has accelerated over the last five years. Since 2017, it has been the leading cause of reported breaches, a trend we expect to continue as hackers maintain a focus on healthcare. The recent rapid digitization of healthcare coupled with legacy infrastructure represent the path of least resistance for hackers.

[1] Source: BakerHostetler: *2019 Data Security Incident Response Report*

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

Through March 2019, more than six million patients have been affected by all types of breaches in healthcare, representing a 76% increase over the number of patients impacted during the same period in 2018. The most common attack vector in healthcare continues to be email. Through the first five months of 2019, over 44% of reported breaches came through email attacks, up from 29% during the same period in 2018. This is a stark reminder that the fundamentals of security remain important. It is critical that every organization develops and executes a continuous cybersecurity training and awareness program for its entire staff. Training end users to be more cautious with email can dramatically decrease your risk profile. This requires changing culture and buy-in from company leadership, but in most situations, investing resources in security awareness and training can have the biggest impact on your cybersecurity posture.

Percent of Breaches via Email [2]



As the number of healthcare entities impacted by breaches continues to rise, it is important that healthcare leaders focus on security fundamentals. Many healthcare organizations find themselves so overwhelmed by the sheer volume of IT and security projects that they end up overlooking the basics of security. Although we know they are critical to lowering our cybersecurity risk, oftentimes patching and security training are the first to fall off the priority list. Allowing your organization to forego these fundamentals to focus on project work could, in fact, be your biggest weakness.

PAUSE TO CONSIDER

1. *Is your security program focused and resourced appropriately to execute the fundamentals?*
2. *Is your organization prepared in the event of a breach?*
3. *Are you executing an adequate cybersecurity training and awareness program organization-wide and tracking high-risk users?*

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

Preparing Your Organization for a Penetration Test

The majority of healthcare organizations have completed a penetration test and recognize the value that a successfully executed test can provide. In order to maximize the value of the penetration test and eliminate any unnecessary burden on your organization, there are a few steps you can take to better prepare your organization.

1. **Remember there is a difference between a vulnerability assessment and a penetration test.** That said, assessing observable vulnerabilities is a big part of the penetration test project. Where the key differences stand out is with the demonstrated impact of those vulnerabilities, as well as the presentation of issues that may not be discoverable by popular vulnerability scanners. Demonstrating impact can strengthen the argument for desired changes and improvements that the network administrator team might be advocating for internally.

2. **Know the network**. One of the biggest challenges a penetration tester encounters is a lack of situational awareness by project stakeholders. It is the responsibility of the penetration tester to design the test to be thorough and the reporting accurate. It is the responsibility of the organization to ensure that the scope (target) is mapped out and documented. This primarily includes identifying subnets that have sensitive devices and determining which teams or departments are responsible for each network segment. This can also aid in swift remediation of identified vulnerabilities and issues reported upon completion of the penetration test.

3. **Understand third-party vendors and service providers.** If an organization has a resource that needs to be tested but it is housed on hardware or in a cloud environment owned by another entity, then permission from that third party is required. This is usually a simple but time-consuming process. Begin that permission process as soon as a penetration test is commissioned and obtain documented approvals before the test starts.

4. **Be honest and transparent.** Penetration testers should be considered an extension of your own team. No matter their approach and tactics, penetration testers are working with your best interest in mind. If there are known issues, report those to the penetration tester assigned to your case. There is value in giving testers the opportunity to discover the issue on their own, but since penetration testers are often pressed for time, sharing that information early in the process can increase efficiency and help address all issues when remediation plans are being developed.

PAUSE TO CONSIDER

1. *Does your organization conduct routine penetration tests?*
2. *During penetration testing remediation activities, do you focus on broken processes or individual issues?*

Comparative Analytics

THE GREAT UNKNOWN

Overall, most healthcare organizations invest more in cybersecurity today than they did a few years ago, but a challenge that remains is how to compare one organization's security posture to another. This is important for two reasons. First, you need to understand what the return is on your investments, as capital tends to be limited and cybersecurity initiatives compete for clinical dollars in most instances. You should be able to demonstrate how investing in cybersecurity has reduced risk and enabled higher quality patient care. Second, based on the principle of reasonableness, current regulation compares one healthcare organization's security program to that of its peers to determine overall effectiveness.[3] So, understanding the maturity of your security program relative to others of similar size and scale is important.

This leaves many healthcare IT and information security leaders asking themselves: is my organization's investment in cybersecurity positively impacting our security posture? Are we allocating our resources in areas that will have the greatest impact on our organization from a risk perspective? How does our security posture compare to that of our peers?

Welcome to the great unknown! Because multiple tools are being used within each security domain and there is no way to aggregate information meaningfully between the tools, it is no surprise that leaders are left with limited ability to provide confident answers to these critical questions.

The missing piece in today's toolset is a unified platform that displays performance across multiple security domains and analyzes how those domains affect each other and contribute to the overall health of your security posture. Without this correlated information, it is almost impossible to get a sense of the big picture or have actionable intel to keep pace with the changing security landscape.

Based on the principle of reasonableness, current regulation compares one healthcare organization's security program to that of its peers to determine overall effectiveness.[3]

The need for advanced peer-based comparative analytics cannot be overstated. Access to these advanced analytics across multiple security domains can show where your security program is excelling and where it needs further improvement to be on par with healthcare organizations of similar size and scale. Additionally, being able to show how both the little wins and the big gains positively contributed to moving the needle in your organization's security posture over time can instill confidence in your team and your security program. It is crucial for leaders to be able to demonstrate a maturing security program over time and to have analytics-powered guidance for allocating resources in areas that will provide the highest ROI, both monetarily and from a security perspective.

PAUSE TO CONSIDER

1. *How are you measuring the progress of your security program?*
2. *Do you know how your security program stacks up to your peer group?*
3. *Are you effectively and consistently providing data to your stakeholders (C-suite, board, etc.)?*

[3] Source: Federal Trade Commission, Data Breach on the Rise: Protecting Personal Information From Harm. Prepared Statement before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, D.C., (Apr. 2, 2014).

How Microsoft Office 365 Is Impacting the Healthcare Industry

Healthcare organizations of every size and scope rely on email as a predominant business tool for both internal and external communications.Unfortunately, email is also a primary vector for network security breaches and cyberattacks. Recent statistics reveal that 92% of all malware is distributed from an email platform, with 93% of all phishing emails housing some type of malware.[4]

Healthcare data is some of the most highly coveted intelligence on the dark web, making it a primary target for cybercriminals on a global scale. It's a trend that is only expected to grow in upcoming years, as an industry review predicted the cumulative number of ransomware attacks within medical enterprises will quadruple by 2020.[5]

Recent statistics reveal that 92% of all malware is distributed from an email platform, with 93% of all phishing emails housing some type of malware.[4]

SCAMS TO PHISH HEALTHCARE EMPLOYEES

Perhaps the most alarming malware statistic within the healthcare industry? A whopping 78% of people understand the risks associated with unknown email links *but click anyway*.[6] Yes, some of these data breaches can be attributed to sheer curiosity or user inattentiveness, and some security lapses stem from users linking their corporate email accounts to outside (unsecured) third-party websites. However, many times healthcare employees are legitimately lured into believing that every communication in their inbox is authentic and secure, particularly if they use Microsoft Office 365 as their primary business collaboration and productivity tool.

As one of the most popular cloud-based business platforms, MS Office 365 often falls prey to a broad spectrum of cybercriminal activity; however, Outlook (its email module) has proven especially vulnerable. Much like other forms of cybersecurity malware, the already turbulent terrain of email threats is continuously (and rapidly) evolving. Hackers on a worldwide scale are designing and executing a wide range of increasingly sophisticated email scams explicitly devised to mimic real-life companies, events, and meetings so recipients will click.

OUTLOOK 365: A POPULAR TARGET FOR GLOBAL CYBERCRIMINALS

These highly complex email attacks aren't just fooling humans—they are also tricking our digital platforms. A recent analysis of MS Office 365 showed that the system demonstrated a "miss rate" greater than 9%, consistently allowing in a diverse range of emails containing the following:[7]

- Phishing
- Malware
- Spam
- Ransomware

From faux board meeting invitations to fraudulent email cards over the holidays, MS Office 365 can inadvertently allow countless hoaxes into users' inboxes, increasing the risk of a data breach with a single mouse click.

CHOOSE THE RIGHT OFFICE 365 SOLUTION TO KEEP YOUR EMAILS PROTECTED

When sourcing specialized providers, it's important to remember that not all outside healthcare cybersecurity services are created alike. Find a specialist that offers a comprehensive suite of strategies and customizable solutions to maximize complete compliance coverage and protection for all of your sensitive stored healthcare data. Key service components should include a wide range of anti-spoofing and link protection tools, such as:

- Email encryption
- Email threat protection
- Email data loss protection
- Uniform information archiving
- Email mobile security

ENABLE MULTI-FACTOR AUTHENTICATION TO MAXIMIZE YOUR SECURITY

Most healthcare organizations recognize the necessity of enabling multi-factor authentication, but some struggle to execute it due to the workflow impact. When putting this best practice in place, it is important to first identify who truly needs access to email outside your environment and who needs access inside the walls of the health system. From there you can determine the most effective way to deploy multi-factor authentication while limiting disruption to your current clinician workflow. Although this security feature may require a bit of a culture change, when deployed correctly, multi-factor authentication can have the biggest impact on your email security program.

Working with an experienced cybersecurity team that delivers agile and robust Microsoft Office 365 solutions can prevent a cyberattack, circumventing suspicious inbound activity to keep your healthcare facility's operations moving forward at maximum momentum.

The good thing about Office 365 is it provides easy access to email for users anywhere in the world. The bad thing about Office 365 is it provides easy access to email for users anywhere in the world. Managing email in a responsible and effective manner means reducing cybersecurity risk while providing the right level of access required for employees to execute their jobs effectively.

PAUSE TO CONSIDER

1. *Have you considered the financial and security implications of giving every user access to email by default?*
2. *Do you have a clear understanding of which users need access to off-premise email, and have you removed external email access to those who don't require it?*
3. *Has your organization implemented multi-factor authentication and geolocation blocking in Office 365?*

[4] Source: https://www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html

[5] Source: https://www.beckershospitalreview.com/healthcare-information-technology/healthcare-ransomware-attacks-to-jump-4-fold-by-2020-5-report-findings.html

[6] Source: https://www.ena.com/phishing-scams/

[7] Source: https://www.darkreading.com/cloud/office-365-missed-34000-phishing-emails-last-month/d/d-id/1330282

Conclusion

Healthcare organizations continue to face threats from multiple threat vectors, but email attacks remain the top weapon of choice. This is a clear reminder of the importance of executing security fundamentals, strong employee cyber-hygiene, and an effective cybersecurity and training program. These threats will likely continue, so start making an investment in your company's cybersecurity culture now. It is critical that healthcare organizations continue to allocate capital toward cybersecurity in order to protect and provide valuable patient care. As IT leaders, it is equally vital for you to measure the progress of your cybersecurity program over time and provide meaningful data to your colleagues and leadership, attesting to the value of your cybersecurity investments and inspiring momentum within your organization.

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).