2019 Horizon Report

THE STATE OF CYBERSECURITY IN HEALTHCARE

Fortified
HEALTH SECURITY

President's Message

Cybersecurity continues to occupy the top priority spot for most healthcare IT teams and is typically one of the top five overall priorities for an entire organization. Because of this, cybersecurity investments are on the same list as clinical investments, competing for the same budget dollars. CIOs and CISOs must now appropriately position cybersecurity investments as a patient safety need and highlight how cybersecurity weaves through every initiative within the healthcare organization.

Providing all stakeholders with visibility into your security program, delivering metric-driven results, and speaking in terms non-security professionals can understand will help you more effectively champion your security program and will likely lead to a better overall view of security within your organization. With the proper understanding and buy-in, healthcare organizations are able to appropriately fund their security programs. While some progress has been made, the majority of healthcare organizations have room to improve.

> Investment in cybersecurity should not be evaluated on a standalone basis. Cybersecurity is a business risk and must be presented and evaluated as such.

Cybersecurity funding is becoming more and more important as our adversaries gain momentum and we face unfavorable market conditions. With double digit increases in reported breaches, we clearly have work to do. On average, a data breach could cost your organization $408 per record[1] and cast a negative impression on your brand. Bad actors continue to focus on healthcare because of the value of our data and the underinvestment in security compared to other industries. These challenges are intensified by the lack of available cybersecurity talent in the market and the burden placed on healthcare organizations from security technology vendors, as most solutions require on-going support to extract maximum value. Alternative approaches exist, and it is important that your security organization is fighting the right battle. Healthcare organizations should evaluate their internal expertise and ability to attract, train, and retain cybersecurity talent. Don't let people be the reason you cannot strengthen your cybersecurity program.

> A data breach could cost your organization $408 per record and cast a negative impression on your brand.

Connected medical devices and IoT (Internet of Things) present a significant risk to most healthcare organizations. The industry is in the early stages of purchasing innovative technology to better secure connected medical devices, and we have an opportunity to do it the right way by establishing programs that encompass people, process, and technology to effectively drive the desired business outcome. Unfortunately, healthcare organizations historically have tended to simply purchase technology to solve a problem, better protect patients, or enable a business initiative, without truly understanding all the required components to effectively operationalize the technology. With limited investment dollars available and patient lives on the line, getting this right is extremely important.

The reason our team produces the Horizon Report twice a year is that we are passionate about our vision to strengthen the cybersecurity posture of healthcare. Sharing data, best practices, and the insights we gain from working with hundreds of healthcare organizations is a cornerstone of one of our core values: collaboration. This passion also shows up in the work we do and in the industry recognition we receive. Thanks to our clients and the work our team achieved this year, Fortified Health Security was recognized by Frost & Sullivan as well as Black Book for our industry leadership in connected medical device security.

My hope is that the Horizon Report builds awareness about threats and provides valuable insight for your cybersecurity 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

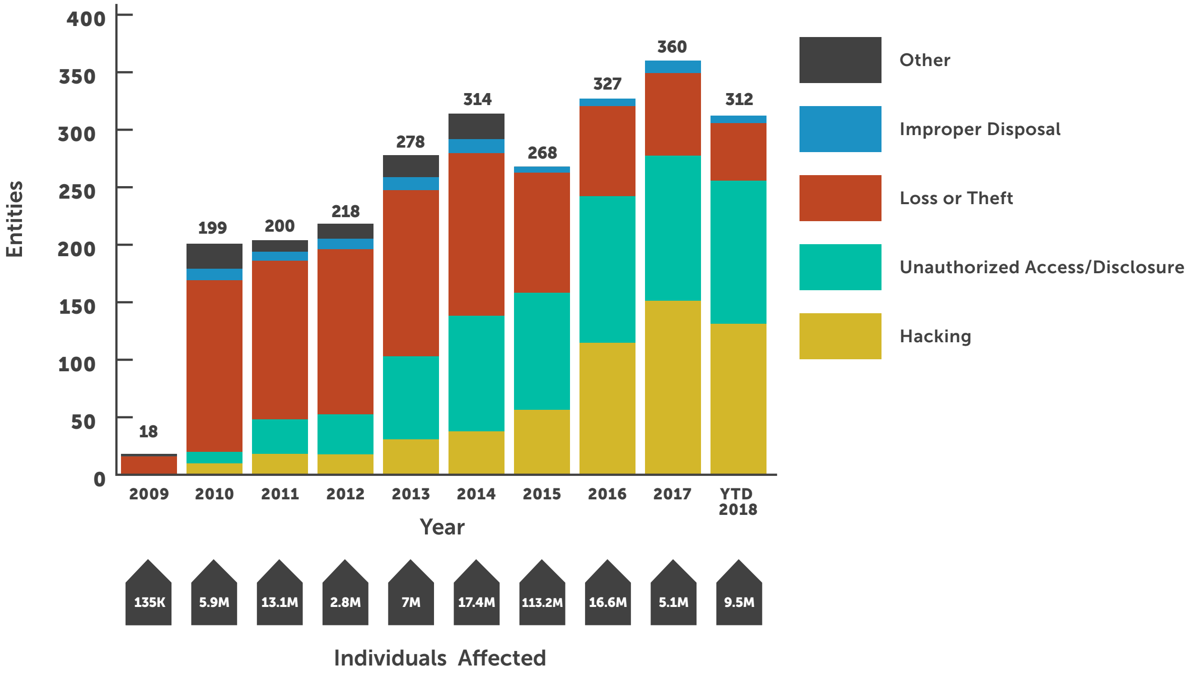
2018 Year in Review

Much like the past few years, the major cybersecurity breach trends in healthcare continued to intensify throughout 2018 and healthcare organizations remain a primary target for bad actors. For the third year in a row, more than 300 healthcare organizations reported a breach of 500+ records and have found themselves on the U.S. Department of Health and Human Services, Office for Civil Rights (OCR)[1] wall of shame.

According to the breach data, healthcare providers continue to be the most targeted and compromised organizations.

Health systems often find themselves overwhelmed with countless IT systems they must manage, a significant number of vulnerable connected medical devices, and resource constraints. Our adversaries understand these challenges and utilize these dynamics to their advantage. Through the first 10 months of 2018, the number of reported breaches has increased by 14% compared to the same period last year. In total, 312 entities have reported a major breach thus far this year, and we expect that number to exceed last year's reported 360. Over 9.5 million individuals have been impacted by these breaches, which is double the number of affected individuals a year ago.

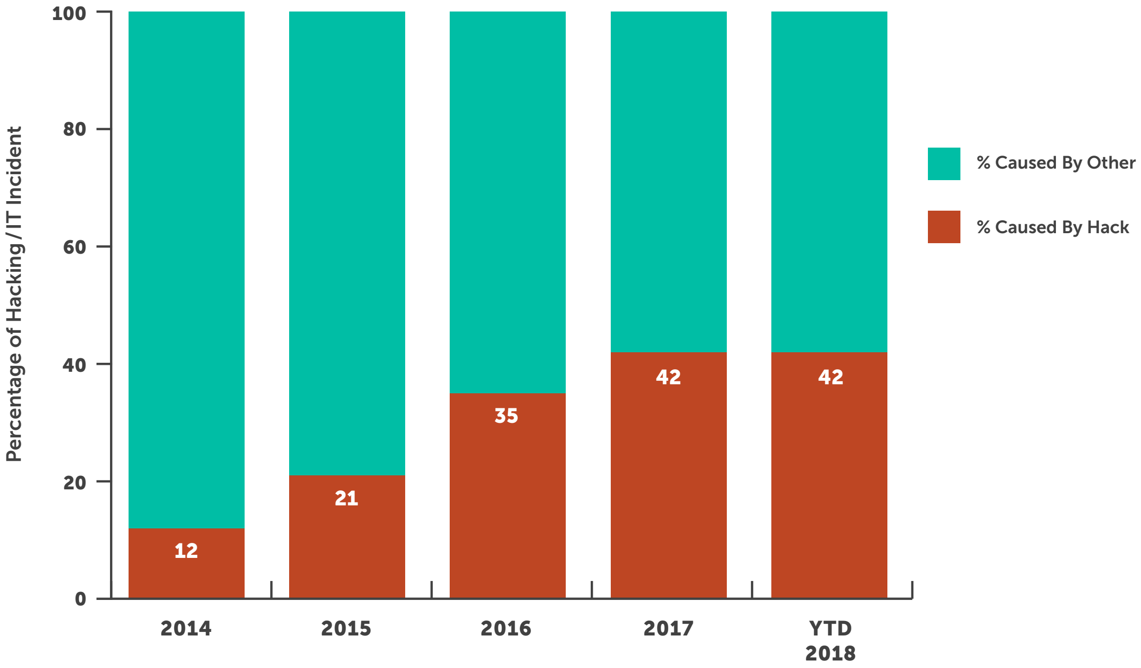
Entities Involved in a Breach



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

Hacking was once again the leading cause of reported breaches in 2018, with over 42% of incidences occurring because of hacking. These successful hacks impacted over 5.7 million people, representing 60% of all affected individuals. This breach data highlights the importance of a "defense in-depth" security strategy, which incorporates a layered approach to security rather than relying on one technology, process, or person.

Breaches Caused by Hacking [2]



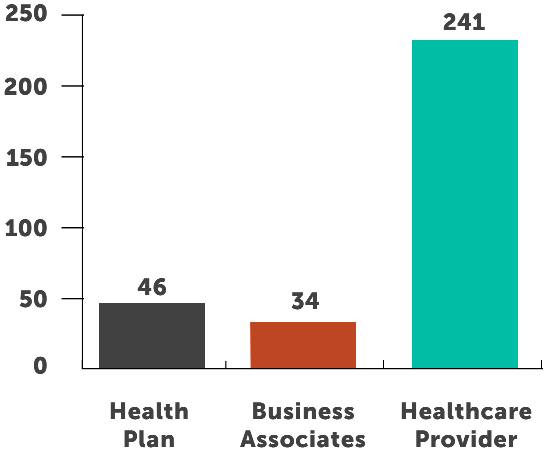
It is imperative that your multi-pronged security program is designed with security fundamentals, anchored in accountability, and driven by discipline. Oftentimes, security teams within healthcare organizations become distracted with special projects or new technology and abandon the daily, weekly, or monthly actions required to continuously execute the appropriate security fundamentals. In many cases, healthcare organizations have poorly implemented technology or lack the expertise to manage sophisticated security tools over time. This is a wide-spread issue magnified by organizations' difficulties in securing adequate resources.

Don't be fooled by the perceived value of technology as your actual level of protection may be less. It may be significantly underperforming expectations, especially if it has not been properly implemented or managed. Making multiple security technologies work in concert with each other and continuously managing them is critical to decreasing your chance of a large-scale breach caused by hacking.

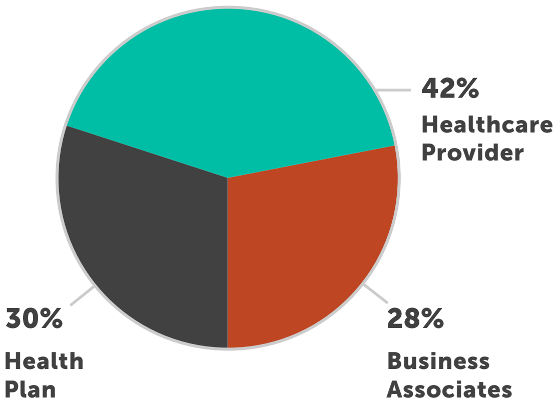
[2] Source: U.S. Department of Health and Human Services Office for Civil Rights

Healthcare provider organizations were the most targeted and successfully breached entities for the 10th year in a row. Over 74% of all reported breaches occurred at provider organizations, down from 80% in 2017. Providers have experienced over 241 breaches this year; we expect that number to climb to over 270 by end of year.

Number of Entities Affected YTD 2018 [2]



Percent of Individuals Affected YTD 2018 [2]



A significant development in 2018 was the number of business associates impacted by a large breach. Thirty-four organizations reported breaches in the first 10 months of 2018, representing a 70% increase over the 20 business associates that reported breaches in all of 2017. This is a noteworthy trend and something health systems should be mindful of as they evaluate their current relationships with third-party organizations.

PAUSE TO CONSIDER

1. *Is your organization prepared for a breach?*
2. *Have you tested your incident response plan?*
3. *Do you have a valid back-up program?*

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

Office
for
Civil
Rights

OCR | Investigations & Fines

2018 marks the largest year of fines issued by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), with a total of almost $25 million. This includes the $16 million settlement paid by Anthem, Inc. for its reported breach in 2015, which eclipses the previous settlement high of $5.55 million paid by Memorial Healthcare System in 2017.[2]

It can take years for OCR to complete its investigation of a reported breach, causing a healthcare organization to spend significant time and resources responding to inquiries throughout the process. Identifying risks is the first step, but building and successfully executing a comprehensive corrective action plan is a requirement in the eyes of OCR. Doing this in tandem with an annual risk assessment based on a proven framework helps expedite investigations.

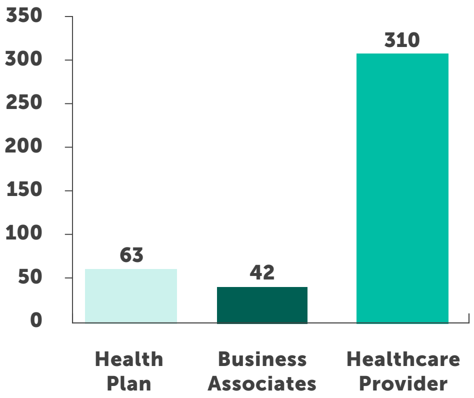
It is important to note that HIPAA is written in such a way that a certain level of interpretation is required; the regulations don't provide black and white guidance on the steps your organization must take to fully comply. Part of the rationale in writing regulations this way is so that a single policy can encompass organizations of all sizes and scale, from billion-dollar health systems to small business associates.

Be sure your organization understands how it will be evaluated or viewed when compared to others in your peer group. The strength of your program will be judged based on acceptable best practices for an organization of similar size and scale. Regional health systems will be compared to other regional health systems, large IDNs to other large IDNs, and small doctor practices to other small doctor practices. This allows for a more reasonable set of accepted security practices based on your organization's market position. You should consider what your peer group is doing with their security programs to ensure you are building, resourcing, and executing a security program that meets your needs. Every healthcare organization is at a different point in its security journey, and what is most important is that you assess risk, identify reasonably anticipated threats, create a plan, and continue to take reasonable action to improve your security posture.

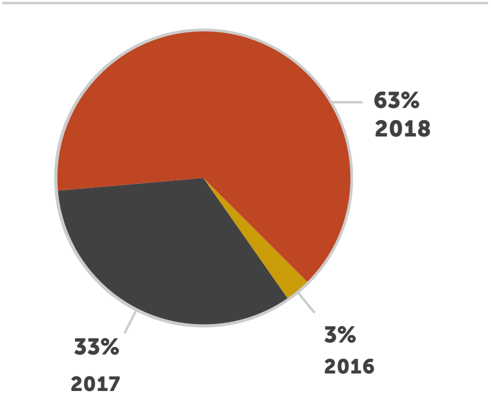
[2] Source: U.S. Department of Health and Human Services Office for Civil Rights

In response to reported breaches, there were 415 active OCR investigations underway at the end of 2018, and 75% of them were with provider organizations. The majority of the investigations were in response to breaches reported in 2018, but 36% of investigations were in response to breaches reported over 12 months ago. The impact of a breach on an organization extends well beyond the initial shock and can leave a lasting impact on your organization. It is important to assess risks annually, execute on security fundamentals, and measure progress over time. As simple as this sounds, many health systems still lack a disciplined approach to managing their cybersecurity posture.

Entities Under Investigation Nov 2018



Date of Reported Breach



PAUSE TO CONSIDER

1. *How does your security program compare to your organization's peer group?*
2. *Is your security program well documented?*
3. *Is your organization making progress on its corrective action plan since your last risk assessment?*

2018 Market Trends

When speaking with healthcare organizations throughout 2018, three major topics consistently came up in almost every discussion:

SECURITY PERSONNEL

Given that the Information Systems Audit and Control Association (ISACA) estimates a global shortage of 2 million cybersecurity professionals by 2019[3], healthcare organizations are struggling to compete for the right resources to execute their security programs.

MEDICAL DEVICE SECURITY

Vulnerabilities related to medical devices is not a new topic, but advances in new technology and an increased threat landscape have many health systems taking steps to better protect their connected medical devices.

HITRUST CERTIFICATION

While numerous health systems have adopted the Health Information Trust Alliance (HITRUST) framework for assessing risk, many are seeking certification to bring validation to their cybersecurity programs.

[3] Source: https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg

THE HUMAN CAPITAL WAR: SECURITY PERSONNEL IN HIGH DEMAND

Attracting, training, and retaining top cybersecurity talent may well be the biggest challenge facing healthcare organizations today as it pertains to building out their security programs. Having access to experienced cybersecurity talent is the foundation of any solid security program because human interaction is required to:

1. **Execute the fundamentals of any security program (e.g., risk assessments, remediation, patching, employee training).**
2. **Maintain and manage advanced security technologies to drive optimal effectiveness.**

Recognizing the importance of people to any successful security program, CISOs and IT leaders across the healthcare industry find themselves squarely in a human capital battle with large corporations from all verticals. Typically, non-healthcare organizations have bigger security budgets, more advanced security technologies, more upward mobility for resources, and higher pay rates. This battle is felt across security staff, from executive leadership to analyst positions, and hits healthcare organizations coast-to-coast.

Executing security fundamentals tends to take a backseat while security leadership focuses on solving the human capital problem. Healthcare organizations may wait to start projects, implement new security controls, or pause the day-to-day execution of their security program altogether until a certain open position is filled. This increases risk and leaves healthcare organizations more vulnerable to attacks. After months of searching, organizations may successfully fill an open position only to find themselves with another hole. Someone else from the security team may have left or the newly acquired team member may not have the expertise required to manage the security tools previously implemented by the organization. This forces organizations to go back to the front lines of the cybersecurity human capital battlefield.

Unfortunately, we expect this battle to intensify in 2019 as demand for cybersecurity resources increases across all verticals and as the threats continue to strengthen. The looming question facing security and IT leadership is “are we fighting the right battle?”

Should your organization continue to fight a battle you may never win or are you better off focusing on patient care and seeking an alternative approach to managing your security program over time? Having a core group of resources to execute certain functions of your security program will certainly always be required, but alternative approaches exist to better equip your network, IT and security teams to tackle the battle you should be fighting: protecting valuable patient data from bad actors. Don’t let your organization’s cybersecurity program stall while you’re focused on human capital because, rest assured, our adversaries aren’t standing still.

PAUSE TO CONSIDER

1. *Are you fighting the human capital battle or are you focused on managing cybersecurity risk?*
2. *Do you have a sufficiently resourced security program focused on the fundamentals?*
3. *Does your current security team have the right expertise to manage the security technologies you have invested in, and are you covered 24/7/365?*

NAVIGATING CONNECTED MEDICAL DEVICE SECURITY

Security risks associated with connected medical devices remain a top concern for leaders in healthcare organizations. Regulatory conversations continued in 2018 and some progress was made to better equip future released devices, but current in-market devices present the largest risk. The Food and Drug Administration (FDA) regulates over 190,000 devices manufactured by more than 18,000 firms in more than 21,000 facilities worldwide.[4]

Many devices already implemented across the healthcare eco-system are largely unpatched, may utilize hard-coded passwords, and run outdated operating systems. These already in-market medical devices provide a massive surface area for attack by adversaries and present the largest risk. Since medical devices do not have a regulated useful life, they typically are not replaced unless they are no longer functioning clinically. This leaves health systems with thousands of potentially vulnerable devices. Segmenting medical devices onto their own network remains best practice, but the speed at which medical devices are connecting to networks is outpacing many organizations' ability to adequately segment these devices.

Besides the challenges that come with a large volume of devices and a great variety of device manufacturers, there is a unique market dynamic between medical device manufacturers and health systems that makes managing the security of connected medical devices exponentially more difficult. Every device manufacturer communicates vulnerabilities differently and some require patches to be pre-approved or the health system risks voiding the device's warranty. The variation in manufacturer processes and devices makes it nearly impossible to resource an effective connected medical device security strategy.

These market dynamics mixed with technical limitations and internal politics present the following challenges for organizations developing a robust cybersecurity program for connected medical devices:

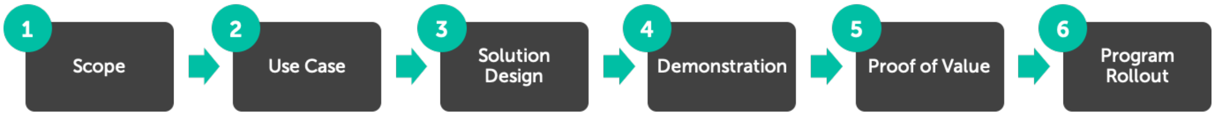
- **Undetermined security responsibility between IT security and clinical engineering**
- **Difficulty achieving timely and accurate asset identification, reconciliation, and remediation**
- **High volume of vulnerabilities and patching to manage at the device level**
- **Security gaps in traditional vendor managed services contracts**
- **Inadequate agent-based security technologies**

Under current regulation, responsibility for in-market device security falls squarely on the shoulders of health systems.

There has been significant progress made with technology focused on securing connected medical devices in the last few years. This is primarily driven by the $100 million in capital poured into a handful of technology vendors that have built solutions powered by machine learning and artificial intelligence to address device security. These companies all differ in features and functionality, but in the simplest form, they successfully identify and profile all the medical devices within your environment. From there, their feature set and security functionality differs greatly.

[4] Source: FDA Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health

We believe the healthcare industry has an opportunity to tackle the challenge of medical device security. That's why we've created a six-step program that aligns people, process, and technology to solve your business problems and drive successful outcomes surrounding connected medical device security. This program is continuous, actionable, scalable, and focused on reducing surface exposure and overall risk.



1

- Assess people, process & technology requirements
- Identify current gaps & challenges
- Understand desired business outcomes
- Establish governance

2

- Develop technology & process use cases
- Align with business needs
- Consider people, process, and technology

3

- Select appropriate technology partner
- Outline process workflows
- Determine on-going management process

4

- Demo technology partner
- Align capabilities with desired business outcomes
- Validate use case enablement
- Determine specific success criteria

5

- Execute technology POV
- Confirm success criteria
- Develop roll-out plan
- Validate business needs are satisfied

6

- Expand program beyond POV site
- Implement process changes
- Roll-out new governance model

Like all major security initiatives, in order to maximize your investment, it is critical to ensure your organization is prepared to operationalize advanced technologies so the business outcome you desire becomes reality.

FORTIFIED HEALTH SECURITY

2018 ACCOLADES

RELEVANT. ACCURATE. BLACK BOOK 2018 UNBIASED SOURCE

FROST & SULLIVAN

2018 BEST PRACTICES AWARD

NORTH AMERICAN HEALTHCARE IOT CYBERSECURITY COMPANY OF THE YEAR AWARD

PAUSE TO CONSIDER

1. *Do you know the actual number and types of medical devices attached to your network?*
2. *Who is ultimately responsible for medical device security, and does that person have the authority to make a difference?*
3. *Do you have the right controls in place to measure and monitor medical device security?*

A CONTINUED JOURNEY TOWARD HITRUST CERTIFICATION

For over a decade, HITRUST has been championing its common security framework (CSF) as a comprehensive, flexible, and efficient approach to regulatory compliance and risk management.[5] The HITRUST CSF is widely adopted in the healthcare industry, and many organizations have embarked on the journey toward HITRUST certification based on an assessment of their security programs. Simply put, the HITRUST CSF is a standard built upon other standards and authoritative sources relevant to the healthcare industry. HITRUST harmonizes existing controls and requirements from standards, regulations, and business and third-party requirements applicable to healthcare. It defines a process for effectively and efficiently evaluating compliance and security risks.

HITRUST offers two assessment types to address an organization's goals and control environment needs. In both types, your organization must be properly scoped to ensure inherent risks are addressed during the assessment.

- **SELF-ASSESSMENT**
  Healthcare organizations may assess themselves against the HITRUST CSF to identify gaps in their current security program. HITRUST certification cannot be granted with this approach.
- **VALIDATED ASSESSMENT (CERTIFICATION)**
  Organizations are measured for compliance with security standards and requirements against the HITRUST CSF.
  - *As part of this process, organizations first complete a self-assessment that is validated by a third-party assessor organization for submission to HITRUST. Assessments meeting or exceeding the current HITRUST program requirements receive a HITRUST-validated report indicating the organization is HITRUST CSF-certified.*
  - *To maintain HITRUST certification, the organization must continue to address corrective action plans within the pre-determined timeframe. Subsequently, in the year following certification, an organization must complete an interim assessment to ensure continuous progress is being made to its security program. Every third year, a full HITRUST assessment must be completed.*

[5] Source: https://hitrustalliance.net/hitrust-csf/

HITRUST certification enables organizations to identify risks through a data-driven approach and develop meaningful action plans to help mitigate these risks. It also can help organizations cut down on the number of vendor-requested risk assessments they must complete annually, as many vendors accept HITRUST certification in lieu of their own risk assessments.

Don't underestimate the lift required to become HITRUST certified. The journey requires significant internal resources, regardless of what any vendor tells you. Our experience is that certification takes an average of 9 months to complete but can be a multi-year process depending on your starting point. Below are some tips to keep in mind when embarking on the HITRUST journey:

1. **GAIN ALIGNMENT ACROSS YOUR ORGANIZATION:**
   Determine the business drivers for becoming HITRUST certified. This helps you gain executive buy-in and ensures that the appropriate level of resources are available.
2. **UNDERSTAND YOUR STARTING POINT:**
   Conduct a very honest and objective review of your security program, including the current documentation and active controls in place. This will help you prepare for the required lift to become HITRUST certified.
3. **PREPARE FOR ORGANIZATIONAL CHANGE:**
   Be aware that HITRUST control requirements are very prescriptive in nature and may require changes to existing security policies within your organization.
4. **RECOGNIZE THIS IS A JOURNEY:**
   Becoming HITRUST certified requires resources, may force changes to your current security program, and may change over time as your organization evolves.

FORTIFIED HEALTH SECURITY IS AN APPROVED HITRUST CSF ASSESSOR

HITRUST
CSF Certified

PAUSE TO CONSIDER

1. *Is HITRUST certification the right option for your organization?*
2. *Is your organization ready to commit to the required changes that may come out of the HITRUST certification process?*
3. *Is your HITRUST initiative resourced appropriately?*

Were We Right?
A Look at Fortified's 2018 Predictions

PREDICTION

Double-Digit Increase in Breaches: Healthcare will experience a 10-20% increase in the number of entities breached, with providers being the most targeted and exploited segment.

So how did we do?

A review of the OCR breach notification data shows the healthcare industry experienced a 13.6% increase in the number of entities reporting breaches over 2017. Between January and October 2017, 360 entities reported a breach versus 312 for the same period in 2018. Healthcare providers represented 74% of reported breaches, an increase of 5%, with 218 provider entities reporting a breach in 2017 and 229 reporting a breach in 2018.[1]

PREDICTION

More Variants of WannaCry Ransomware: In May 2017, many companies around the world fell victim to the WannaCry ransomware attack. Other variants of WannaCry (like NotPetya) soon followed. With unpatched systems still prevalent and vulnerable to WannaCry, it is safe to assume hackers will release additional, more intelligent variants of WannaCry in 2018.

So how did we do?

The vulnerability itself still threatens unpatched and unprotected systems across the country. According to ESET LiveGrid®[6], variants of WannaCry are still being detected.

PREDICTION

Breaches due to Business Associate Neglect (Third-Party Risk Management Failure) on the Rise: In 2017, OCR has identified at least 18 breaches due to business associate neglect and, more importantly, failure by the covered entity to manage that risk. Healthcare-covered entities will continue to experience risk and possible breaches in 2018 unless effective business associate risk management programs are established.

So how did we do?

In 2017, 5% or 18 of the 360 reported breaches included business associates. This quadrupled in 2018 to 24% of reported breaches, or 74 of the 312 at the time of this report. This staggering increase highlights the importance of managing business associate risk.[1]

PREDICTION

Increased Threat to IoT Devices: Medical devices constitute a large number of Internet of Things (IoT) devices currently connected to healthcare networks around the world. In October 2017, newer, more powerful versions of IoT malware ("Reaper" and "IoTroop") were discovered in the wild. The malware spreads very easily through IoT devices with little to no security. We should expect this malware to be seen in more healthcare IoT devices in 2018 — if they're not there already.

So how did we do?

A survey conducted by CHIME and KLAS in October reported that 18% of provider organizations had medical devices impacted by malware or ransomware.[7] The number of ICS-CERT medical device advisories per year is estimated to double from less than 20 in 2017 to almost 40 in 2018.[8]

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

[6] Source: https://www.welivesecurity.com/2018/05/10/one-year-later-eternalblue-exploit-wannacryptor/

[7] Source: https://chimecentral.org/chime-klas-survey-measures-providers-confidence-in-medical-device-security-programs/

[8] Source: https://www.medcrypt.co/medcrypt-vulnerability-analysis-whitepaper-1.pdf

Users — The Last Line of Defense!

As healthcare IT teams face limited budgets, resource constraints, and difficulty defending their networks against escalating threats, security vendors continue to claim to have the "silver bullet" to solve all your problems. Before evaluating the next security technology solution, we recommend you focus internally, as there is one constant: employees are your biggest security risk. It is important to take steps to protect your organization from employee actions, whether malicious or accidental.

It is commonly said that people, or users, are an organization's most important asset, and yet they are almost impossible to secure because…

YOU CAN'T PATCH THEM

- New variants of social engineering aimed to manipulate them into divulging confidential or personal information are continuously evolving.
- They are bombarded with email communication.
- Their security habits vary between their home life and work life.

YOU CAN'T RECONFIGURE THEM

- Habits are habits. They are very hard to break.
- A culture shift is difficult to influence enterprise-wide.
- You can't add non-impactful security controls that will burden or hinder their clinical workflows.

YOU CAN'T HOLD THEIR HANDS

- Processes/tools vary throughout the organization.
- It's difficult to protect or influence all users.

Industry best practice recommends considering people, process, and technology when implementing safeguards to protect users from themselves. But, where should you begin?

User hygiene is the most important control you can put in place. This starts with an effective security and awareness program. Establishing an effective program is more cultural than financial. It is important that user education is championed by top leadership and transcends throughout every layer of the organizational chart.

Our experience has shown that gamification in the implementation of your security and awareness program provides immediate results as the competitive nature of individuals always seems to bubble to the top. The program should be multi-faceted and not just a point-in-time training course or email blast. The components of a well-rounded program are outlined below. Some are much easier to implement than others and most can be operationalized at minimal cost. It is the necessary culture change that is typically the major roadblock at most healthcare organizations.

NEW EMPLOYEE ORIENTATION

- Make employees aware of the security risks in your organization.
- Provide a communication mechanism when they see a threat.
- Instill a sense of trust and action from security.
- Offer visibility into the security controls in place.

ANNUAL SECURITY TRAINING

- Obtain executive support.
- Select modules that cover the biggest security risks.
- Ensure you test and capture metrics.
- Do not make it a laborious effort for users.

PHISHING – CONTROL/TRAINING

- Test the enterprise regularly.
- Make it competitive within organizational departments.
- Use current threats when designing your campaign.
- Provide instant feedback to users.

THREAT INTELLIGENCE

- Use threat intelligence from your security team.
- Create and communicate a threat dashboard.
- Provide users visibility to the controls in place.

PERIODIC COMMUNICATION

- Propagate threat information to ALL users.
- Create security news bulletins or alerts.
- Provide additional references for information.
- Increase awareness during high-threat times (i.e., holidays, Tax Day, Black Friday).

Your users are busy in their day-to-day work, serving patients and providing care. Therefore, effective cybersecurity programs must implement technologies that detect and stop threats before they reach users in the first place. Implementing the right security technologies in conjunction with your security and awareness program is how you mitigate these risks to an acceptable level. This next step can require additional investment in people, process, and technology, so it is important that you first maximize the functionality of all security technologies previously implemented.

Email and web browsing are the top platforms used by cybercriminals to breach your organization's data. The available technologies are plentiful, and you need to choose them carefully based on your organization's risk reduction goals. It's also important to make sure you have the resources to manage and monitor them, as none are turnkey or "set it and forget it" technologies.

Below is a list of technology categories that support a well-rounded security program. Determine which technologies you need to address risk in your organization based on recent risk assessments, audits, previous security incidents, and/or breaches.

ENDPOINTS

- Web Reputation
- Ransomware Protection
- User Behavior Monitoring
- Application Control
- Data Loss Prevention
- Encryption

WEB FILTERING

- URL Filtering
- Malware Protection
- Spyware/Grayware Protection
- Bot Detection

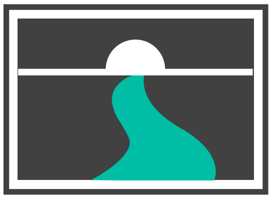
EMAIL SECURITY

- Antivirus Protection
- Phishing Protection
- Spam Protection
- Business Email Compromise Protection
- Anti-Malware Protection Utilizing Predictive Machine Learning
- Malicious Attachment Sandboxing

Like all security-related initiatives, it takes dedication, support, and a willingness to change organizational culture to successfully protect users. Keep in mind that security is a journey and incremental improvement is best. Work with your organization to drive the right culture change, and you can successfully lower risks associated with user behavior.

PAUSE TO CONSIDER

1. *Is your security and awareness program a point-in-time solution or does it drive ongoing engagement?*
2. *Have you defined success for the security and awareness program, and are you publicly sharing results?*
3. *Is everyone engaged in your security program from executive leadership to physicians and staff?*



Looking Ahead

CYBERSECURITY OUTLOOK 2019

1

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.

2

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.

3

INCREASED THREAT FROM CRYTOPMINING

Cybercriminals are exploiting known vulnerabilities to steal the processing power of these devices to mine for cryptocurrencies. Crytpomining continues to rise as cybercriminals are not content with only stealing data like they once were. We expect this threat to increase in 2019. [9]

4

CONTINUED TARGETED PHISHING ATTACKS

Today it is estimated that 90%[9] 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.

[9] Source: https://enterprise.verizon.com/resources/reports/dbir/

Moving Forward

MAKE VISIBILITY KING

You can't protect what you can't see. Creating a security program that is powered by technology and appropriately operationalized can give you the visibility you need to better protect your organization. Visibility will ultimately lead to better protection and lower overall risk.

PRACTICE LEAST PRIVILEGED ACCESS

This is very difficult in healthcare due to the dynamic clinical user base. Organizations that practice least privileged access management significantly change their risk profile when the process is powered by technology and successfully supported.

OPERATIONALIZE YOUR TECHNOLOGY

Healthcare executives often look for a silver bullet, which forces organizations to purchase technical point solutions that tend to be under-implemented and under-supported. This leads to the misperception that you are more protected than you are. Don't forget to consider how you monitor and manage technology over time.

IMPLEMENT AN INFORMATION SECURITY PROGRAM

Compliance is not security. However, a properly implemented security program usually meets compliance. Healthcare organizations should focus on creating a "defense in-depth" strategy that is adequately supported and grounded in an approach that encompasses people, process, and technology.

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 Security 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).