2017 MID-YEAR
Horizon Report

THE STATE OF CYBERSECURITY IN HEALTHCARE

Fortified HEALTH SECURITY

fortifiedhealthsecurity.com | 615-600-4002 | 2555 Meridian Blvd Suite 250, Franklin, TN 37067

President's Message

In 2017, the U.S. healthcare industry has been experiencing many cybersecurity-related threats, including one massive ransomware attack which might have negatively impacted patient care at many hospitals across the nation if a security researcher had not found and pulled the "kill switch." Of course, I am referencing the WannaCry ransomware attack that occurred on May 12th, spread to over 150 countries and impacted over 300,000 devices.

As an industry, healthcare faces a significant uphill challenge when it comes to safeguarding sensitive patient data. Cybersecurity threats and malicious actors continue to focus on exploiting patients by compromising their personal health information and endangering their care by significantly disrupting hospital operations, as other countries experienced with WannaCry.

The healthcare industry faces a significant uphill challenge in safeguarding sensitive patient data.

This single attack caused many healthcare IT organizations to spend the weekend — or weeks, in some cases — deploying a critical security patch that Microsoft issued on March 14th, almost two months prior to the attack. Organizations that were still running older, unsupported versions of Microsoft Windows were initially at risk until they released an emergency security patch for these older platforms as well.

This threat was one that could have been avoided by following the fundamentals of a strong cybersecurity program. This attack forced many healthcare organizations to take steps they may have previously neglected because of technical, clinical, financial or political reasons. But, in the moment of crisis, many organizations overcame these challenges and pushed through the fear of the unknown or an unstable infrastructure by deploying a patch to fix the vulnerability. We all know that this isn't a long term strategy and that it's likely a similar crisis will occur if the organization's cybersecurity infrastructure isn't addressed. But what would have happened if it had been too late? What if your organization's decision to knowingly avoid a critical fundamental to any cybersecurity program had led to the turning away of patients? What if you had been exploited?

Organizations must focus on cybersecurity fundamentals and avoid chasing new technologies.

Organizations must now focus on laying a solid cybersecurity foundation, rather than simply chasing the newest technologies. Unfortunately, there is likely no simple fix, as these are very complex and complicated issues that must be prioritized within your organization. The time has come for healthcare leaders to truly understand the current cybersecurity posture of their organization and remove barriers that may prohibit your organization from executing the fundamentals.

Cybersecurity threats at their core are patient safety risks and, frankly, the stakes are too high. My hope is that the Horizon Report builds awareness about threats and provides you valuable insight. We welcome your feedback and perspectives at horizonreport@fortifiedhealthsecurity.com. Enjoy.

Regards,

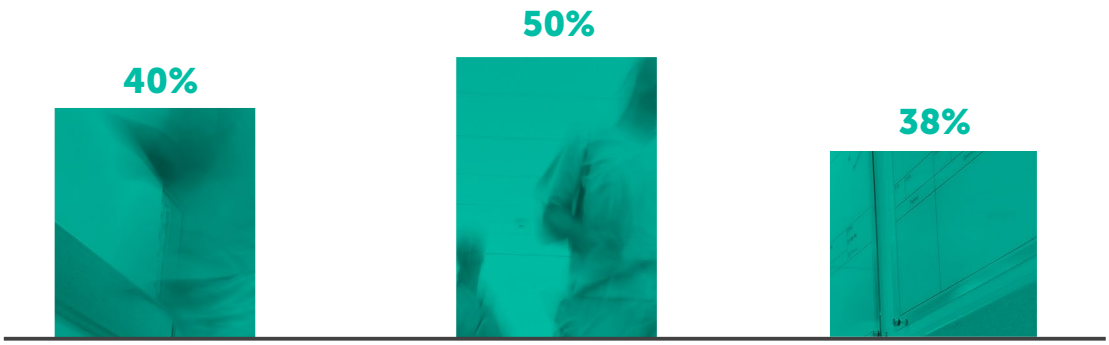
Dan L. Dodson

2017 Mid-Year in Review

It took only three days for the first data breaches of a health plan in 2017 to be reported to The U.S. Department of Health and Human Services' Office for Civil Rights (OCR). It was only five days until a healthcare provider first reported a breach of over 500 patient records, according to the OCR Wall of Shame. This just so happens to be one day faster than in 2016, but this sends the same chilling message: there is still a ton of work to be done to better protect personal health information.

These breaches are coming at a time when patients are starting to act more like consumers. This forces healthcare organizations to guard their reputations, develop strategies for better patient engagement, and provide increased amounts of sensitive data to multiple interconnected devices. Recognizing the potential impacts of a breach on an organization before one occurs is important as many health systems only start investing in cybersecurity after they have been negatively impacted by an incident and, at that point, it may be too late for some patients. Reports* suggest that nearly forty-percent of consumers would abandon or hesitate using a health organization if it is hacked. Fifty-percent of consumers would avoid or be wary of using a medical device if a breach was reported and thrity-eight percent would be wary of using a hospital associated with a previously hacked device.

Recent breaches come as patients are increasingly acting more like consumers — forcing healthcare organizations to guard their reputations while developing better patient engagement strategies, and adopting and securing multiple interconnected devices as a part of evolving patient care.



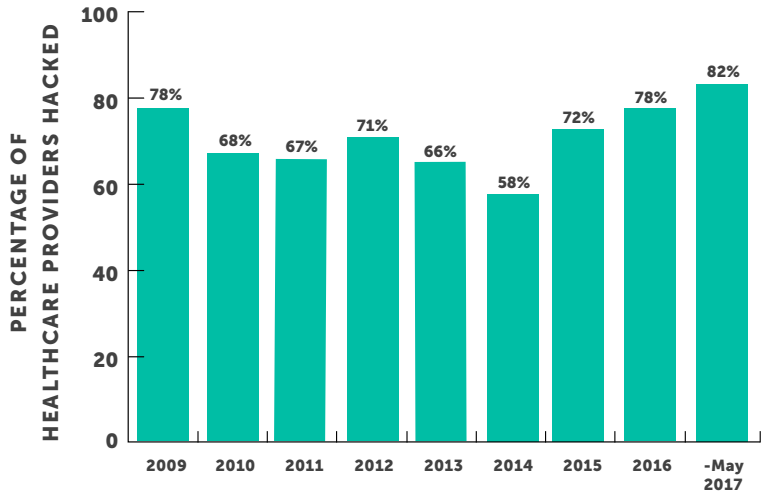
If breached, a healthcare organization's patient engagement initiatives and perhaps their revenue (if it causes a decrease in patient volume) may be significantly impacted due to public perception. However, the potential impact of a breach could be even greater for medical devices due to their direct interaction with patients. While no hacked medical device is known to have caused patient harm to date, the ramifications to the healthcare industry due to this type of breach could be catastrophic. The good news is that some healthcare organizations are starting to recognize the potential risks associated with medical devices and are prioritizing their security.

*Source: Top health industry issues of 2016: Thriving in the New Health Economy, PwC Health Research Institute

According to one poll, twenty-three percent of healthcare organizations stated that lax security on devices is their biggest concern which ranked second only to mobile device hacking which twenty-nine percent cited as their highest priority for 2017. Overall, fifty-eight percent of healthcare organizations ranked Internet of Things (IoT) device security, which includes connected medical devices, a high priority for 2017.*

Regardless of the attack vector, an organization that experiences a significant reportable breach could be in for a big drop in patient confidence. Unfortunately, the number of healthcare entities that reported a significant data breach over the past twelve months has increased almost nineteen percent over the prior twelve-month period. The increase in entities impacted by a breach was largely driven by the healthcare provider segment as they experienced over thirty percent increase during those periods. Healthcare providers continue to be the biggest target and experience more breaches than health plans and business associates combined.

In fact, every year since 2009, healthcare provider entities have represented the largest percentage of reported breaches and that percentage has grown every year since 2014.



The potential impact of ransomware on the operations of a health system caught the attention of most healthcare leaders and gained significant traction across the C-suite as a direct result of the WannaCry attack. For many, this made cybersecurity real to them for the first time. This exploit wreaked havoc in Europe and directly impacted patient care at multiple NHS facilities, as some hospitals were forced to turn patients away and cancel appointments. This attack impacted multiple verticals but, for some people in healthcare, it brought a sense of reality to the true risks of cybersecurity and potential impacts on patient care.

*Source: 2017: The Year Ahead in Health Information Technology, Healthcare IT News

Ransomware is malicious software which blocks access to computer systems and data on network shares until a sum of money is paid. WannaCry is a brand new type of ransomware that is being deployed through remote exploits. WannaCry ransomware infections stopped operations for dozens of hospitals in the UK. The cyber attack has hit more than 300,000 computers across 150 countries since the initial release. The attack vector anatomy was comprised of the following factors:

- The exploits used in the attack were drawn from exploits stolen from the National Security Agency.
- The attack works by remotely exploiting a vulnerability in SMB to get a foothold on vulnerable machines. No user interaction is required to perform this attack.
- Unpatched Windows machines were exploited and then infected with WannaCry.
- Because of its success infiltrating systems, the WannaCry ransomware is already inspiring imitators. At least four variants thus far have been identified.

WannaCry hit more than 300,000 computers across 150 countries since the initial release.

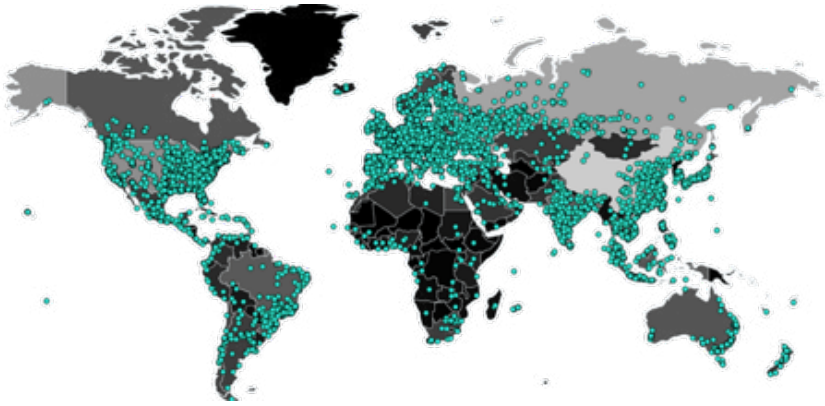
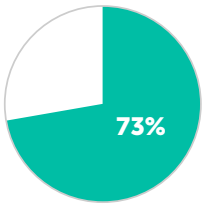


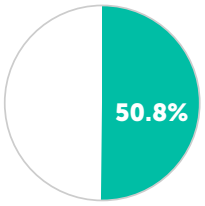
Figure III – *A breakdown of the locations that were affected by the WannaCry attack*

The only guaranteed solution to prevent this attack was for healthcare systems to make sure all the Windows security updates were installed, specifically MS17-010 which was released in March 2017. Due to the ferocity and span of this attack, Microsoft has released out-of-band updates for operating systems it stopped supporting, such as Windows XP, Windows Server 2003, and Windows 8. Furthermore, we recommend health systems use the "principle of least privilege," by giving only read/write permissions on critical network shares to the smallest number of users possible.

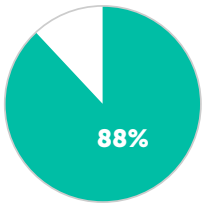
RANSOMWARE'S TOLL ON THE HEALTH INDUSTRY



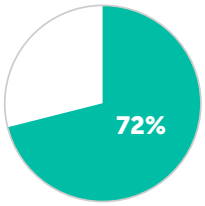
Percentage of healthcare organizations that have a business continuity plan in place in case of a ransomware attack.



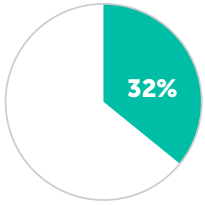
Percentage of providers who say they would not pay a ransom to get a patient's data back.



Percentage of all ransomware attacks on U.S. companies in 2016 that were tied to the healthcare industry.



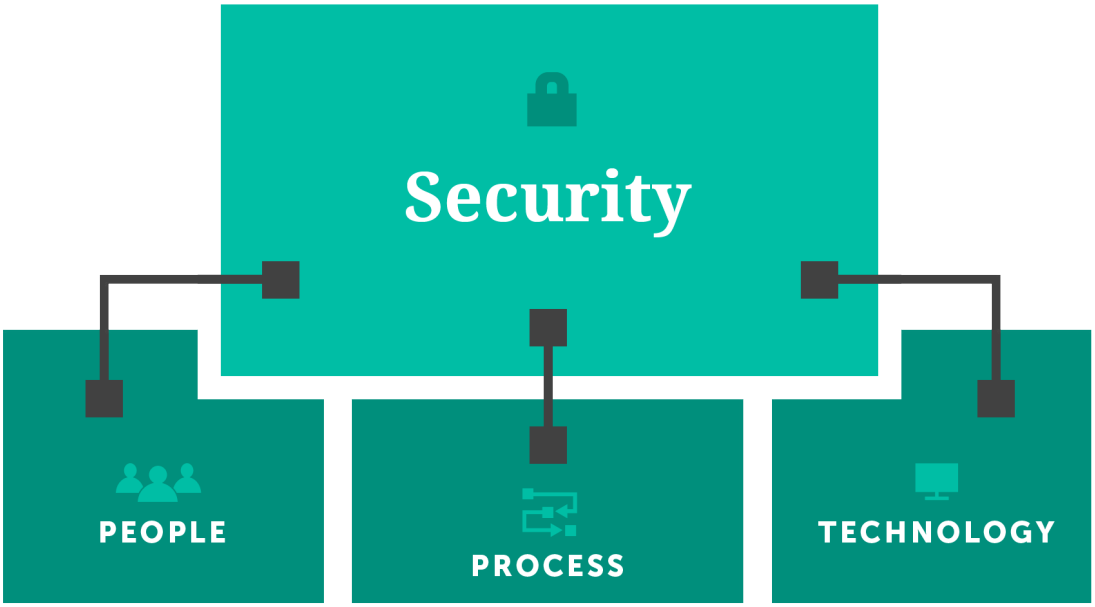
Percentage of infected business users who could not access their data for at least two days following a ransomware attack.



Percentage that lost access for five days or more.

Source:

(Modern Healthcare, 6/20/17)



The best prevention against WannaCry or any attack are proactive security measures around people, process and technology. A defensive in-depth strategy will position your organization with a multi-layered, multi-faceted approach that will reduce your surface exposure exponentially.

The best prevention against any attack is proactive security measures around people, process & technology.

The "People" factor must be addressed and continuously measured in order to increase effectiveness. Educating your employees/users on threats to your organization, safe web browsing practices, the hazards of clicking embedded links or opening attachments in unverified emails, and to scrutinize emails before opening them are just some of the basics. Your users are your first line of defense to prevent successful attacks and/or breaches.

In order to take your user's education to the next level, you should conduct simulated phishing and social engineering exercises and campaigns. This will give your users "real world" experience in dealing with such attacks. Social engineering is still the most effective way that malicious individuals are able to access sensitive information. In fact, a recent survey "Nuix's The Black Report: Decoding the Minds of Hackers" found that employee training was still a primary obstacle to hackers:

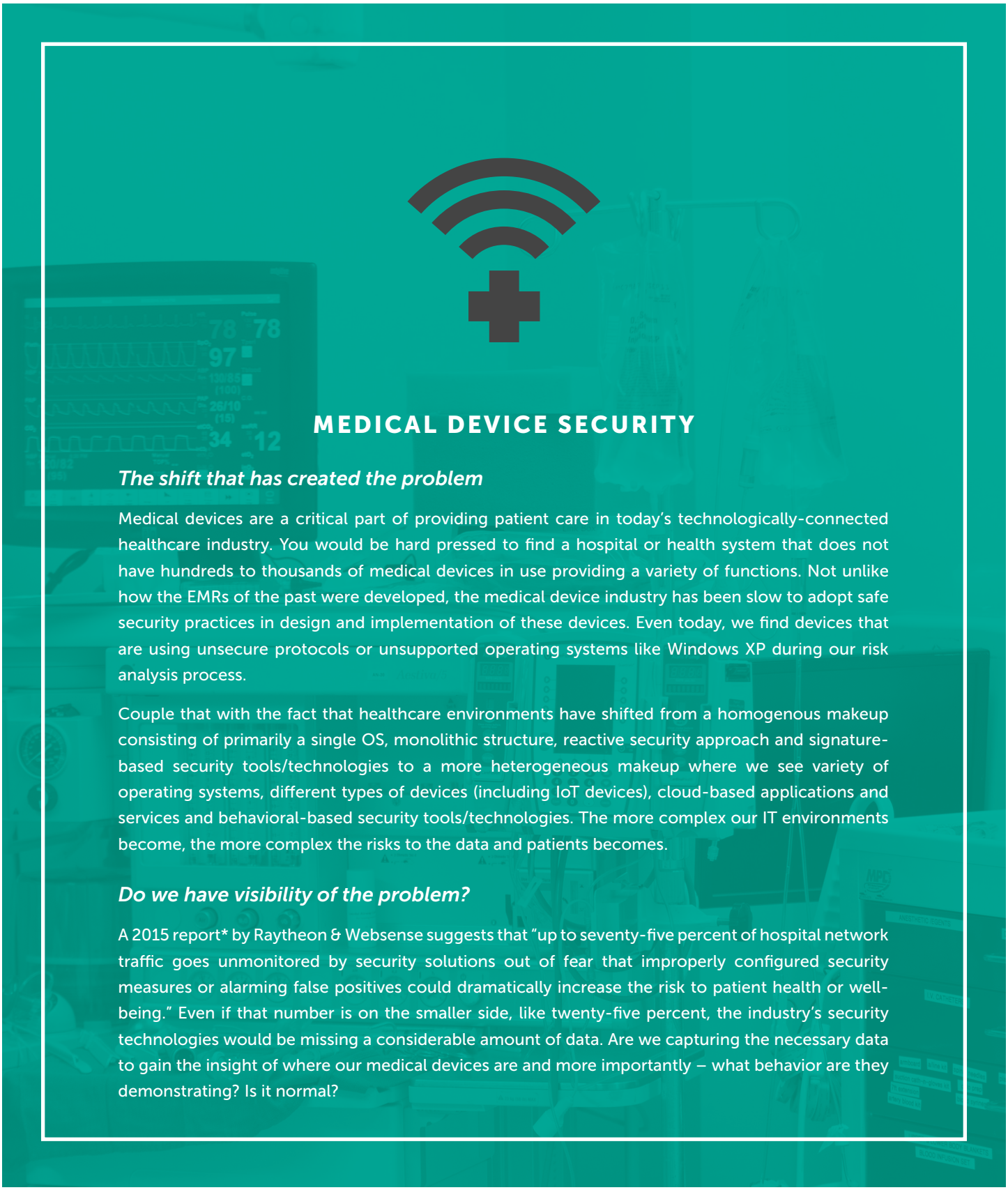
"What was interesting was, security countermeasures that historically organizations think are effective, the hackers laugh at and blow right by," Pogue says. "And then other things that organizations don't want to spend money on—like employee training—the hackers are like, 'The most difficult thing for us to get around is well trained people.'"

*Source: https://sm.asisonline.org/Pages/Hacking-Culture.aspx

The second facet of the defense in depth revolves around Process. In general, the processes around backups, incident response, breach notification, and disaster recovery should all be considered when strengthening a security program. For this particular scenario, the basic process that could have prevented an outbreak within your organization was a patch or vulnerability management. The patching of MS17-010 when it was released in March of this year would have closed the gap. Now we understand that is easier said than done. Some applications may "break" if patched due to unstable infrastructure or configuration, whereas other concerns revolve around high availability, making a reboot almost impossible. To tackle this, it is critical that organizations develop a multi-phased vulnerability management process. Deploying patches in a phased or tiered approach will help alleviate concerns that have kept patching from being a systematic, repeatable process – especially when a test environment is not present.

Technologies such as Security Information and Event Monitoring (SIEM), Data Loss Prevention or Intrusion Prevention Systems (IPS) can be leveraged to identify and even react to a ransomware attack as it is happening. We have seen that custom policy and rulesets can be utilized to alert in real time that there is something awry within the operating environment. Additionally, Network Access Control (NAC) platforms could make the isolation of infected devices quicker and easier.

Similarly, to the WannaCry attacks in May, the world experienced another massive cyber-attack in June; Petya. This attack caused numerous issues for healthcare organizations across the U.S. A Hospital in West Virginia was forced to rebuild all their computer hard drives as they were unable to access data and they needed to provide clean access to their EMR. Nuance Communications, a major provider of dictation services, was also impacted by the attack which impacted physician documentation across the country. The impact of these attacks serves as another reminder of how the fundamentals of a cybersecurity program are so crucial to protecting patient data.



MEDICAL DEVICE SECURITY

The shift that has created the problem

Medical devices are a critical part of providing patient care in today's technologically-connected healthcare industry. You would be hard pressed to find a hospital or health system that does not have hundreds to thousands of medical devices in use providing a variety of functions. Not unlike how the EMRs of the past were developed, the medical device industry has been slow to adopt safe security practices in design and implementation of these devices. Even today, we find devices that are using unsecure protocols or unsupported operating systems like Windows XP during our risk analysis process.

Couple that with the fact that healthcare environments have shifted from a homogenous makeup consisting of primarily a single OS, monolithic structure, reactive security approach and signature-based security tools/technologies to a more heterogeneous makeup where we see variety of operating systems, different types of devices (including IoT devices), cloud-based applications and services and behavioral-based security tools/technologies. The more complex our IT environments become, the more complex the risks to the data and patients becomes.

Do we have visibility of the problem?

A 2015 report* by Raytheon & Websense suggests that "up to seventy-five percent of hospital network traffic goes unmonitored by security solutions out of fear that improperly configured security measures or alarming false positives could dramatically increase the risk to patient health or well-being." Even if that number is on the smaller side, like twenty-five percent, the industry's security technologies would be missing a considerable amount of data. Are we capturing the necessary data to gain the insight of where our medical devices are and more importantly – what behavior are they demonstrating? Is it normal?

*Source: https://www.insight.com/content/dam/insight-web/en_US/article-images/ebooks/Partner/2015-industry-drill-down-report-healthcare.pdf

Who owns the problem?

With an increasing number of connected medical devices, medical IT networks are becoming more complicated. Typically, neither the IT department nor the Clinical Engineering teams within a healthcare organization have the necessary visibility and risk assessment tools, making the unprotected medical devices one of the weakest spots in a medical facility's infrastructure. The lack of clear definition surrounding who owns the problem (CE vs. IT) has produced a situation where one of two things happens:

1. **One party assumes that another party is addressing medical device security**
2. **Both parties are working in parallel without any cross-communication which results in wasted effort and possibly one party's efforts counteracting the others'**

What can we do to address the problem?

THE FIRST AND HARDEST STEP in addressing these security-related issues is gaining visibility. Gaining the required situational awareness and visibility is two-fold. The first is insight into what devices are operating within your environment. This is by far the most difficult to overcome. Our experience has shown that we typically can't get two people in the same organization to agree on how many devices are connected in their environment. What makes it so hard is the dynamic nature in which devices are introduced and removed from the environment. It is imperative that organizations develop processes to gain the required visibility in order to gather actionable intelligence based on the associated risk. The next part of the visibility equation is acquiring the situational awareness into what vulnerabilities each unique device presents to the operational environment. Much like gaining the insight into which devices are on your network, organizations need to develop and implement processes to discover and validate vulnerabilities to their medical devices. Unfortunately, it doesn't stop there. Once validated vulnerabilities are identified, the organization must evaluate the associated risk. Only then can decisions be made about the appropriate actions to address the risk.

THE SECOND STEP is the establishment of clear lines of ownership and communication. As previously mentioned, medical devices seem to live between the IT department and Clinical Engineering. To best address the management of these devices, the management/ownership needs to fall squarely on one department's shoulders with the latter acting in a supporting role. Unfortunately, we can't tell you who that department should be because each organization is unique in its allocation of resources (people, time, funding). In turn, the organization needs to make that decision based on their individual circumstances but it is critical that the decision is made and it is clear.

A THIRD consideration in addressing medical device security is compensating controls. Since the manufacturers are still playing catch-up with addressing the security portion of their devices it is critical that healthcare organizations institute compensating controls to reduce the identified risk or close the known vulnerabilities of medical devices. This could come in the form of a logical network separation or security technologies with unique controls that harden the environment in which the medical devices operate.

THE FOURTH is leveraging technologies where appropriate to automate the management of medical devices. Thankfully, the industry is now starting to see technologies come to market that can accomplish the work outlined above in a more efficient and automated fashion. The investment into a technology that can gain an organization visibility into the devices on their network and their associated vulnerabilities (where risk can be ascertained) and assist in remediating will provide tremendous value in closing the security gaps with regards to medical devices.

OCR UPDATE

So far in 2017, OCR announced the first ever HIPAA settlement based on the untimely reporting of a breach of unsecured PHI as well as the first ever settlement involving a wireless health service provider. While these are firsts from an OCR settlement perspective, both may have been avoided if basic Risk Assessments had been completed and the appropriate policies and procedures implemented.

The first OCR settlement underlines the importance of policies and procedures including those that address the time requirements for Breach Notification. OCR's investigation revealed that the health system failed to notify, without unreasonable delay and within 60 days of discovering the breach, each of the 836 individuals affected by the breach, prominent media outlets (as required for breaches affecting 500 or more individuals), and the OCR.

The second settlement highlights that not understanding HIPAA requirements creates risks, as this entity was unable to produce final policies and procedures during OCR's investigation. Some were not fully implemented while others were still in draft form including those regarding the implementation of safeguards for ePHI.

OCR has continued to pursue settlements aggressively and is on pace to almost double the amount of settlements in 2017 as compared to 2016. Through the first five months of 2017, OCR has reached over $17M in settlements compared to just over $23M in full year 2016. Furthermore, OCR has already reached nine settlements thus far this year compared to 13 in all of 2016.

Private-Public Collaboration

HEALTH CARE INDUSTRY CYBER SECURITY TASK FORCE

For over a year the Health Care Industry Cybersecurity Task Force (Task Force) has been charged with developing a Report outlining the growing challenges the healthcare industry faces when securing and protecting itself from cybersecurity incidents. The 21-member Task Force was the result of the Cybersecurity Act of 2015 (the Act) and is comprised of top professionals from across the industry (providers, payers, device manufacturers, security professionals, federal agencies, etc.) both private and public sector. As part of the Act, Congress asked the Task Force to accomplish six tasks:

(A) Analyze how industries, other than the healthcare industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) Analyze challenges and barriers private entities (excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) Review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) Provide the Secretary with information to disseminate to healthcare industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the healthcare industry;

*Source: "Report on Improving Cybersecurity in the Health Care Industry"

"Covered entities must not only make assessments to safeguard ePHI, they must act on those assessments as well," said OCR Director Jocelyn Samuels. "OCR works tirelessly and collaboratively with covered entities to set clear expectations and consequences."

"Covered entities need to have a clear policy and procedures in place to respond to the Breach Notification Rule's timeliness requirements," said OCR Director Jocelyn Samuels. "Individuals need prompt notice of a breach of their unsecured PHI so they can take action that could help mitigate any potential harm caused by the breach."

(E) Establish a plan for implementing title I of this division, so that the Federal Government and healthcare industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

(F) Report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

On June 2, 2017, the Task Force released the "Report on Improving Cybersecurity in the Health Care Industry" (the Report) to Congress fulfilling the statutory mandate. The Task Force collected 151 potential risks (68 confidentiality risks, 30 availability risks, 30 integrity risks, and 23 patient safety risks). Fifty-five percent of these potential risks related to the loss of Protected Health Information (PHI) which Covered Entities and Business Associates are charged to protect under HIPAA regulation.

The detailed Report can be found on the Fortified Health Security website under resources.

Report Findings

The Report paints a clear picture of a complex industry that has rapidly digitized in the last ten years with many interconnected data points running on an outdated infrastructure creating a wide surface area for cyber-attacks. The balance between providing real-time data to physicians at the point of care in a minimally disrupted manner, coupled with the charge for interoperability, has left the healthcare market more connected and more vulnerable to attacks than ever before.

Furthermore, the Report states that most healthcare organizations lack sufficient financial resources, struggle with retaining in-house information security expertise, don't have the infrastructure to identify and track threats – much less analyze and take action based on the information — and are likely running unsupported legacy systems that cannot easily be replaced. These challenges are only exemplified by the fact that most health systems run on single digit margins forcing some organizations to choose between funding critical patient care or cybersecurity initiatives. These dynamics, combined with the increased sophistication of bad actors, have the Task Force portraying a healthcare industry in need of immediate action. The Report identifies six imperatives along with 27 recommendations and 104 action items. The imperatives are:

1. **Define and streamline leadership**, governance, and expectations for healthcare industry cybersecurity.
2. **Increase the security and resilience** of medical devices and health IT.
3. **Develop the health care workforce capacity** necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. **Increase healthcare industry readiness** through improved cybersecurity awareness and education.
5. **Identify mechanisms to protect** R&D efforts and intellectual property from attacks or exposure.
6. **Improve information sharing** of industry threats, risks, and mitigations.

The Report calls for the implementation of all recommendations to increase awareness, better manage threats, reduce risk and vulnerabilities, and implement protections not widely adopted across the healthcare industry. While all the recommendations in the Report provide value to the cybersecurity posture of healthcare, and we encourage you to read the entire Report, there are several themes that caught our attention.

1. Create a cybersecurity leader role within HHS to align industry-facing efforts for healthcare cybersecurity*

The Report suggests that there should be a single leader responsible for coordinating all healthcare cybersecurity programs and initiatives both within and outside of the Department of Health and Human Services (HHS). The recommendation is that The Health Care Cybersecurity Leader would work within HHS, externally with other federal agencies that impact healthcare, and with other healthcare related groups. The general premise is that this approach would reduce duplication of efforts and provide clarity, as well as better guidance around cyber risk and threats.

Given the diversity and complexity of the healthcare eco-system, which must support not only patient records but medical devices, this approach would allow one individual to look at cyber risks more comprehensively and be positioned to have a greater impact on the overall risk to the industry. Having the right individual charged with the coordination of initiatives across multiple government agencies which impact healthcare cybersecurity and balancing the ever-changing threat to PHI would likely increase our ability to respond as an industry and lead to an overall reduction of cybersecurity risk as an industry.

2. Establish a consistent, consensus-based, healthcare-specific Cybersecurity Framework**

The Report suggests that a single cybersecurity framework be build upon the minimum standard of security required by the NIST Cybersecurity Framework and the HIPAA Security Rule. Although the NIST framework is not healthcare-specific, it does provide a solid foundation for assessing cybersecurity risk and combing the HIPAA Security Rule with NIST would provide a comprehensive framework for accessing healthcare specific risk.

Sources

**"Report on Improving Cybersecurity in the Health Care Industry", Recommendation 1.1*

***"Report on Improving Cybersecurity in the Health Care Industry", Recommendation 1.2*

Taking the step to provide a single framework would enable a unified lexicon for the healthcare industry as well as provide unified standards, guidelines, and best practices. This would make the management of cybersecurity risk across the entire healthcare spectrum much more manageable and measurable. As predicted by Fortified in the 2016 Horizon Report, this Report further encourages the move to a National Cybersecurity Framework specific to healthcare.

3. Secure legacy systems*

The Report defines legacy systems as those which may not have ongoing support from the hardware and software vendors to include both legacy medical devices and legacy EHR applications. The specific action item to healthcare delivery organizations regarding securing legacy systems outlines some best practices that should be adopted for all products.

The Report recommends that health delivery organizations :

- inventory their clinical environments and document unsupported operating systems, devices, and EHR systems;
- replace or upgrade systems with supported alternatives that have superior security controls where possible;
- develop and document retirement timelines where devices cannot yet be replaced;
- leverage segmentation, isolation, hardening, and other compensating risk reduction strategies for the remainder of their use.

4. Establish a Medical Computer Emergency Readiness Team (MedCERT) to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures**

Network connected medical devices represent a significant vulnerability for most health systems as outlined later in the Horizon Report — so much so that the Report frames this recommendation up as an interest of national security. The Report also describes "**a market dynamic whereby healthcare providers have shouldered an inordinate amount of the burden even when actions needed to improve security in the device have been outside their control.**"

MedCert would be comprised of experts including hardware, software, networking, biomedical engineers, and clinicians to enable a deep understanding of patient safety implications of medical device vulnerabilities. The team would be a trusted

**Sources*

**"Report on Improving Cybersecurity in the Health Care Industry", Recommendation 2.1*

***"Report on Improving Cybersecurity in the Health Care Industry", Recommendation 2.6*

entity charged with determining the "ground truth" regarding medical device vulnerabilities and proposed mitigations. If needed, this team could be deployed into the field to investigate a suspected or confirmed medical device compromise. Given the potentially widespread and inherent impact to patient safety that an exploitable medical device vulnerability represents, the idea of creating a unified, proactive team of experts that would be at the ready represents a giant step forward.

5. Every organization must identify the cybersecurity leadership role for driving for more robust cybersecurity policies, processes, and functions with clear engagement from executives*

Although some organizations may already have a Chief Information Security Officer (CISO) on the team while others may not, the focus for this recommendation centers around accountability and responsibility. Many organizations still view cybersecurity as an IT problem and have very poorly-defined roles and responsibilities for their cybersecurity leader. We experience this situation often with health systems and encourages organizations to empower the cybersecurity leader to implement a robust cybersecurity program including an appropriate level of oversight and enforcement.

The Task Force calls for a "unified effort – among public and private sector organizations of all sizes and across all sub-sectors – to work together to meet an urgent challenge. They also reflect a shared understanding that for the healthcare industry cybersecurity issues are, at their heart, patient safety issues." There is hope that all the work that took place over the last year simply represents the beginning of a much-needed collaboration between the public and private sectors to advance healthcare beyond our adversaries.

*Source: Report on Improving Cybersecurity in the Health Care Industry", Recommendation 3.1

CONCLUSION

Cybersecurity threats at their core are patient safety risks. The stakes are high and if you wait until after a breach or attack to take action, it's already too late. The time has come for healthcare leaders to truly understand the current cybersecurity posture of their organization and remove barriers that may prohibit their organization from executing the fundamentals. The best prevention against any attack is a proactive security strategy built around people, process and technology. Investing in and promoting an organization-wide, culturally-driven approach to cybersecurity will greatly reduce risk and, most importantly, ensure consistent patient care.

We hope this Mid-Year Horizon Report starts you on your path "from compliance to confidence" as we say at Fortified Health Security. Developing a strong cybersecurity posture does take time, energy and teamwork, and we welcome your feedback and perspectives at *horizonreport@fortifiedhealthsecurity.com*.

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

sales@fortifiedhealthsecurity.com

OFFICE
2555 Meridian Blvd., Suite 250
Franklin, TN 37067

ABOUT THE AUTHORS

Dan L. Dodson is President of Fortified Health Security where he brings over 10 years' experience in the healthcare and insurance industries — serving as both an operational leader and sales leader. Dan's specific focus has been in aligning organizational strengths with client needs through the execution of relevant go-to-market strategies and solution development. Dan also serves as an Executive Vice President for Santa Rosa Consulting. Prior to joining Fortified, Dan was Senior Vice President at Hooper Holmes, Inc. (AMEX: HH), a company serving the health and wellness and life insurance industry. Prior to joining HH, Dan served as Global Healthcare Strategy Lead for Dell Services (formally Perot Systems) and has held numerous positions within various healthcare organizations including Covenant Health System and The Parker Group. Dan holds an M.B.A. in Health Organization Management and a B.S. in Accounting and Finance from Texas Tech University.

Ryan Patrick is a Vice President of Fortified Health Security where he focuses on increasing client security posture through driving collaboration between sales and operations teams. Prior to joining Fortified, he served as the Deputy Chief Information Officer for the New York State Division of Military and Naval Affairs and as a Director of a Security & Privacy healthcare IT consulting practice, in addition to working in the information security office for organizations such as MetLife and Memorial Sloan-Kettering Cancer Center. He currently holds an M.B.A. from Norwich University, the Certified Information Systems Security Professional (CISSP) certification and is a HITRUST Common Security Framework (CSF) certified practitioner.

ABOUT FORTIFIED HEALTH SECURITY

Fortified Health Security is a leader in information security, compliance and managed services, focused exclusively on helping healthcare professionals overcome operational and regulatory challenges everyday in regards to HIPAA, HITECH, and Meaningful Use. Founded in 2009, Fortified has established a heritage of excellence, compliance and innovation. Today, Fortified partners with healthcare organizations across the continuum, serving health systems, single hospital entities, physician practices, post acute providers, payors and business associates. *www.fortifiedhealthsecurity.com.*