2018 MID-YEAR
Horizon Report

THE STATE OF CYBERSECURITY IN HEALTHCARE

Fortified HEALTH SECURITY

President's Message

The U.S. healthcare industry continues to experience breaches at an unprecedented rate with bad actors working tirelessly to exploit our systems, extract our data, and sell it for monetary gain. Thus far in 2018, we have seen attack momentum increase and new hacking groups formalize with greater sophistication and focus than ever before. For example, a new attack group dubbed Orangeworm hit the scenes earlier this year and deployed an exploit to select organizations, including several in the healthcare industry. We expect to see more targeted attacks like this as our adversaries continue to narrow their focus.

...We have seen attack momentum increase and new hacking groups formalize with greater sophistication and focus than ever before.

While we have made progress in some areas and, as an industry, continue to invest in cybersecurity programs, typically most healthcare organizations aren't allocating enough capital to keep up with the attackers. Given tight budgets, competing internal priorities, and overall financial pressures, it is imperative that healthcare organizations make every dollar count. I strongly encourage organizations to remember that training and awareness should be the cornerstone of any solid cybersecurity program, as cyber-attack prevention and defense starts with people. Also, we must be ever mindful of the operational costs associated with advanced security technologies.

The demand for cybersecurity experts is at an all-time high, and healthcare organizations must compete against all industries for top talent.

The demand for cybersecurity experts is at an all-time high, and healthcare organizations must compete against all industries for top talent. This means many are often forced to fight a human capital battle during the cybersecurity war. Stay focused on large-scale goals, so you don't become distracted with the daily push to attract, retain, and manage a massive team of cybersecurity experts. Your organization will always need people, but I would encourage you to think critically about the best way to allocate resources, so you can effectively manage your cybersecurity program and ensure your actual and perceived values of these resources are equal. I often see healthcare organizations get caught up in the battle and lose the war while spending big dollars. Don't let your prior investments be improperly managed, or you may find yourself disappointed.

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

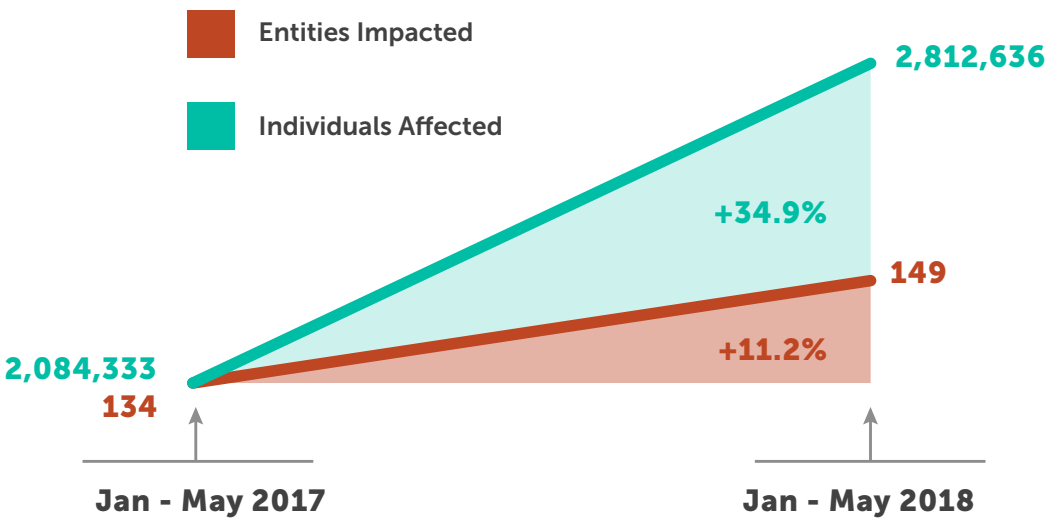
2018 Mid-Year in Review

Healthcare organizations remain a massive target for cyber-attacks, and the preferred attack methods from 2017 continue to be used in 2018, including targeted phishing campaigns and ransomware attacks. Email attacks have accounted for almost 28% of all reported breaches thus far in 2018, up 3% from last year. The bottom line is that we must work as an industry to better educate end users on how to identify, avoid, and report malicious emails. People remain the top cause of cybersecurity vulnerability.

Provider organizations have been compromised more this year than health plans and appear to be more heavily targeted.

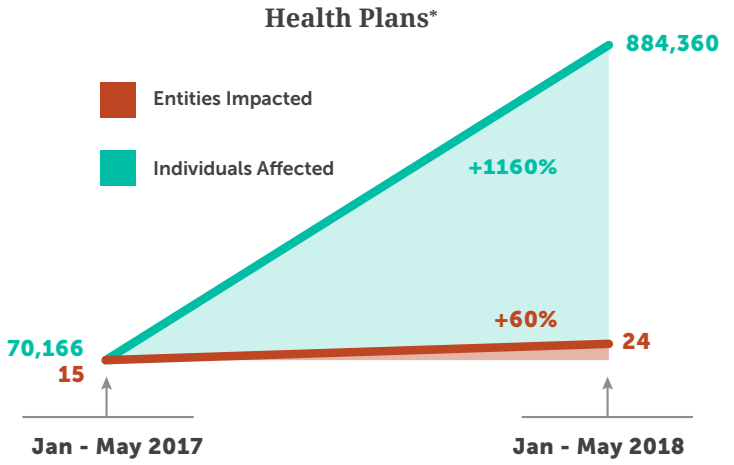
According to the U.S. Department of Health and Human Services Office for Civil Rights (OCR), this has been the case since 2009. The OCR Wall of Shame also found that in the first week of 2018, there were four major breaches containing more than 500 patient records. This is the same number of breaches reported in the first week of 2017, but the momentum has increased from there. Through the first five months of 2018, there have been 149 breaches reported with over 2.8 million patients impacted, as compared to 134 breaches impacting 2.0 million patients during the same period in 2017. This represents an 11% increase in the number of entities affected and a 35% increase in the number of individuals affected.

Total Market (U.S.)*

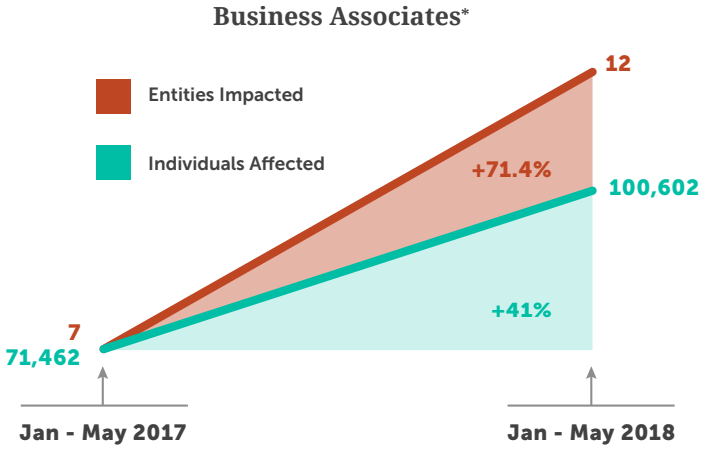


*Source: U.S. Department of Health and Human Services Office for Civil Rights

Although the total percentage of breaches affecting providers is more than the total percentage affecting health plans and business associates combined, the number of reported breaches by health plans and business associates has significantly increased through the first five months of 2018. Health plans have reported 24 breaches so far this year compared to 15 during the same period in 2017, representing a 60% increase in the number of entities impacted. The total number of patients impacted by those breaches increased by more than 1,000%. Additionally, of those health plans impacted by a breach thus far in 2018, 38% were either state or city-affiliated health plans.



There have been 12 breaches reported by business associates in 2018, as compared to seven during the same period in 2017, representing a more than 70% increase in the number of business associates impacted. The total number of patients impacted by those breaches increased by more than 40%.



The breaches healthcare organizations have experienced thus far in 2018 highlight the importance of deploying a comprehensive cybersecurity risk management program that takes into account people, processes, and technology. As cyber thieves continue to focus on the human element to successfully exploit healthcare organizations with email phishing attacks, it is important to implement ongoing cybersecurity training and awareness programs that scale your entire organization.

*Source: U.S. Department of Health and Human Services Office for Civil Rights

U.S. FOOD & DRUG ADMINISTRATION

FDA MEDICAL DEVICE SAFETY PLAN

Connected medical device security continues to be a high-profile topic among healthcare providers and device manufacturers. The Food and Drug Administration (FDA) currently regulates more than 190,000 devices manufactured by more than 18,000 firms. Many in-market devices are already network-connected, and the majority of new devices will connect in some form or fashion to enable data exchange. In April, the FDA released its **Medical Device Safety Plan** in which regulators laid out a framework for improving device safety throughout the entire product life cycle. The Plan focuses on how the FDA can:

1. **Establish a robust medical device patient safety net in the United States**
2. **Explore regulatory options to streamline and modernize the timely implementation of post-market mitigations**
3. **Spur innovation toward safer medical devices**
4. **Advance medical device cybersecurity**
5. **Integrate the Center for Devices and Radiological Health (CDRH) pre-market and post-market offices and activities to advance the use of a total product life cycle (TPLC) approach to device safety**

As it relates to cybersecurity, the Plan proposes several measures to mitigate and prevent breaches of connected devices. These include: 1) considering a requirement for firms to update and patch device security in product design and submit a "Software Bill of Materials" to the FDA, 2) updating pre-market guidance on medical device cybersecurity, 3) considering a new post-market authority that requires firms to adopt policies and procedures for coordinated disclosure of vulnerability, and 4) exploring the development of a CyberMed Safety (Expert) Analysis Board (CYMSAB).

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

FILLING IN THE GAPS

While the Plan is well-intended and addresses certain aspects of the risks associated with connected medical devices, there are several gaps that still need to be addressed. Specifically, the Plan does not adequately account for the sheer volume of medical devices that are already on the market. It is widely understood that most health system CFOs are unlikely to approve capital spend for medical devices that are still "functional." This dynamic, coupled with no regulated useful life for devices, means that there are hundreds of thousands of connected medical devices that are running unpatched, outdated software and are vulnerable to an attack. These devices must be considered to truly understand the overall cybersecurity posture in the healthcare industry. Secondly, the Plan doesn't adequately prepare for the future of cybersecurity. The threat landscape continues to evolve and, therefore, our policy must create an environment ready for change.

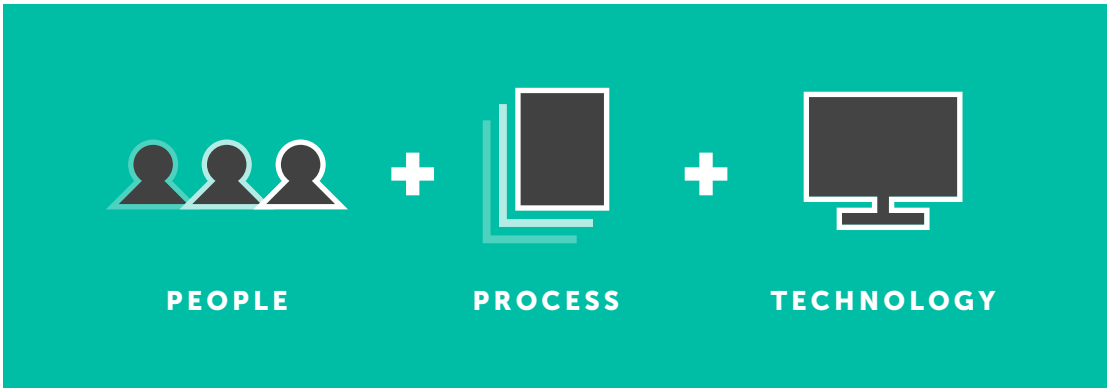
Until the FDA and HHS (and the OCR) get on the same page and force manufacturers to take security seriously and, more importantly, hold them accountable, the industry will continue to struggle and the risk of catastrophic failure will increase. The sad fact is that medical device manufacturers don't have to really worry about building security into their product design because the industry needs their products. There is currently no consumer demand to build security into products from the ground up. Individually, healthcare organizations can't influence the manufacturers to do the right thing. Additionally, there is no singular body that represents the industry and can advocate for change. The responsibility falls squarely on the government agencies that require healthcare organizations to protect their patients and patient information.

The FDA or the OCR needs to be empowered to levy fines against poor product design and/or maintenance when manufacturers fail to account for security. Hospitals and their business associates are required to protect patients and their information from long-term effects of a breach. However, if compromised, manufacturers have no official regulation or consequence. OEM companies need to be held to the same standards and expectations of their healthcare customers, or we will continue to struggle to see real progress and improvement.

Historically, the healthcare industry and its partners have been slow to adopt new technologies and concepts. Usually, it takes a significant emotional event (like a breach) for these initiatives to gain traction. The industry doesn't want to deal with the aftermath of failing to secure the very devices that keep people alive. **The FDA's Plan only focuses on the current problem, which is a great start, but fails to address how we'll tackle the unknowns of the future.**

The Plan includes a task force to react to outbreaks of compromised medical devices, but where is the prevention strategy? Where is the task force that will look ahead to anticipate new threats and attack vectors with in-market devices or new devices that are still going through the FDA approval process?

While regulation continues to evolve, some providers have made significant strides in the last couple of years. Many organizations are actively working to develop and implement comprehensive medical device security programs to help mitigate risks for their current connected devices. These programs should consider people, processes, and technology to effectively coordinate, monitor, and impact security risks associated with these devices.



ARTICLE CONTRIBUTED BY
DIGITALGUARDIAN®
www.digitalguardian.com

3 STEPS FOR IDENTIFYING & PROTECTING PATIENT INFORMATION

HEALTHCARE DATA BREACHES ARE FREQUENT AND LARGE

According to the OCR, the top 10 healthcare data breaches in the last five years have exposed more than 122 million patient records, and more than 9 million additional records were disclosed in breaches still under investigation.[1] These breaches have consequences for the covered entities as well as the individual patients.

For example, the OCR can order financial penalties for violations. In 2017, it ordered more than $19 million in fines, including $5.5 million from Memorial Healthcare Systems for the disclosure of PHI of over 115,000 patients, $3.2 million from Children's Medical Center of Dallas for the disclosure of electronic PHI, and a $2.5 million settlement from CardioNet for the impermissible disclosure of PHI.[1] This year, Fresenius Medical Care North America was fined $3.5 million for five separate breaches.[1]

STEP ONE:
DISCOVER WHERE PHI RESIDES AND WHEN IT'S AT RISK

The obvious first step in protecting PHI is to discover where it resides in your environment. Data discovery software identifies where PHI is located and where it's at risk by scanning and inspecting all content at rest in servers and endpoints.

One area that is prone to accidental or malicious data disclosure is shared repositories that are accessible to large numbers of legitimate users, such as file shares and Microsoft SharePoint. Scanning these for patient record numbers and other PHI using a low-privilege guest account makes it possible to quickly identify and close a common security gap.

[1] **Source:** https:/ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=7AD924D8387021727C5957A9FBAB6910

STEP TWO:

APPLY AUTOMATED CONTROLS TO PROTECT PHI

The discovery of PHI is the essential first step, but discovery alone won't mitigate the risk of leakage or breaches. Automated, effective controls must then be applied to prevent inadvertent or deliberate leakage, using the same systems that discovered the data. This can take many different forms, including automatic encryption when data is emailed or moved, blocking data movement to unauthorized locations or devices (cloud storage, public email, removable storage devices, etc.), or requiring an approval process and login when special circumstances require waivers. Many healthcare organizations are reluctant to turn on these automated controls for fear of impacting caregivers. But the best data loss prevention solutions available today can provide granular controls that don't impact legitimate patient data handling.

STEP THREE:

EXPAND EFFORTS TO COVER ALL SENSITIVE DATA

The discovery and protection of sensitive information doesn't end with PHI, but must encompass all sensitive data that's stored and processed by your organization. Privacy laws are expanding across the world, and many healthcare organizations are subject to these new regulations. For example, the European Union's General Data Protection Regulation's (GDPR) definition of personal data is more expansive than the Health Insurance Portability and Accountability (HIPAA) PHI standard. The Payment Card Industry Data Security Standard (PCI-DSS) covers personally identifiable information (PII) and credit card identifiers. Even organizations not covered by specific standards are not safe from legal action. The U.S. Federal Trade Commission (FTC) has brought action against organizations after data breaches under Section 5 of the FTC Act, arguing that consumers have an expectation that personal information provided to those organizations would be protected by "reasonable" security practices. The same technologies and services that can assist with PHI discovery and protection are designed to identify and protect all sensitive data in any format across the enterprise and the cloud.

A PROVEN PROCESS

This three-step process – discover, control, and expand – is proven to deliver both quick wins in the short term and a more mature security posture that reduces your organization's breach and regulatory risks.

NIST FRAMEWORK INTRODUCES SUPPLY CHAIN MANAGEMENT CATEGORY

On April 16, 2018, the National Institute of Standards and Technology (NIST) released[2] the much-anticipated Version 1.1 of its Cybersecurity Framework, which included one new category and several new subcategories addressing a number of topics, such as: authentication and identity, cyber risk self-assessments, supply chain cybersecurity management, and vulnerability disclosure. "This update refines, clarifies and enhances Version 1.0," said Matt Barrett, program manager for the framework, in the release. "It is still flexible to meet an individual organization's business or mission needs, and applies to a wide range of technology environments such as information technology, industrial control systems and the Internet of Things." Version 1.1 is fully compatible with Version 1.0 and is designed to be used by new users as well as current users.

> "[Version 1.1] is still flexible to meet an individual organization's business or mission needs, and applies to a wide range of technology environments such as information technology, industrial control systems and the Internet of Things."
>
> **- MATT BARRETT, PROGRAM MANAGER, NIST**

The biggest change for healthcare organizations utilizing the framework is the introduction of a supply chain management category under the Identify function. This new category brings with it five new subcategories addressing topics such as: supply chain risk management processes, suppliers and third party information systems, business contracts, supply chain member assessments and audits, and response/recovery planning and testing. This is an area that is not necessarily intuitive on exactly how and where healthcare would assess and capture risk.

In speaking with our clients, we have found there is some confusion on where a hospital or business associate can fall within the supply chain from an information systems perspective. Unfortunately, there isn't a silver bullet answer that would cover all types of organizations in the industry, but here are a few areas to consider when identifying threats to confidentiality, integrity, or availability of services and data:

- Utility companies providing power to the organization
- Medical devices that are unable to be maintained or patched by the vendor
- Cloud-based EHR systems (or other cloud-based critical applications/services) that are dependent on external connectivity and availability of their hosted platform
- Third party vendors/business associates that don't have access to sensitive data but have administrative access to your network

The new version recognizes that U.S. national and economic security depends on the reliable function of critical infrastructure.

[2]**Source:** https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

CONCLUSION

Hackers continue to pose threats to healthcare operations and have impacted some organizations' ability to serve patients. The volume of attacks has continued to increase across all industries which has further strained the ability for healthcare organizations to attract the right level of cybersecurity expertise. These challenges are likely to continue for years. It is paramount that healthcare organizations allocate capital and resources in areas that have the biggest impact on their security posture. It is important that we look for alternative ways to fight the cybersecurity war and not get lost in the cybersecurity human capital battle.

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 helps healthcare organizations effectively develop the best path for their security program based on their unique needs and current situations. 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 the Global Healthcare Strategy Lead for Dell Services (formally Perot Systems), and has held positions with 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. He has also spoken at leading industry 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.

Ryan Patrick is a Vice President at 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 and 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 holds an M.B.A. from Norwich University, as well as 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 cybersecurity, compliance, and managed services, focusing exclusively on 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 to 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. *www.fortifiedhealthsecurity.com*