# 2018 Horizon Report

## THE STATE OF CYBERSECURITY IN HEALTHCARE

Fortified
HEALTH SECURITY

# President's Message

Many Americans knew of cybersecurity breaches prior to this year, but the large-scale impact of the Equifax breach of 2017 put them on the map for most of us. From dinner table to conference table, the breach started numerous conversations about protecting personal information. In turn, it caused many organizations to re-evaluate their cybersecurity program. Just as the Enron scandal of the early 2000s triggered a change in accounting standards, experts predict that, over time, this breach will have a significant impact on regulation. The attention the Equifax breach generated will no doubt impact how patients (consumers of healthcare) view organizations that have been hacked. One report suggests that over 40 percent* of consumers would abandon or hesitate to use a health organization if it had been hacked. Even if that number were 5 or 10 percent, many healthcare organizations could not survive the financial ramifications associated with declining patient volume.

One report suggests that over 40 percent of consumers would abandon or hesitate to use a health organization if it had been hacked.

Unfortunately, healthcare leaders are stuck in the crosshairs of consumers and hackers. While consumers require transparency, access to information and assurance that their personal health information will remain safe, hackers are busy compromising patient information at a faster speed than ever before. As healthcare IT organizations strive to become more accessible and "open" to support patient engagement initiatives, hackers continue to target and exploit healthcare organizations for monetary gain. The required investment in cybersecurity is often overlooked or under-funded until an incident occurs. At that point, the damage to your organization's reputation may have already occurred.

Healthcare organizations must strike a balance between enabling patient engagement initiatives and securing patient data. While there is no simple fix to this complex challenge, healthcare organizations often focus on the wrong areas at the wrong time. Organizations must develop and execute the fundamentals of security first before exploring advanced solutions. This requires a defensive, in-depth approach to cybersecurity that is grounded in a detailed HIPAA Security Risk Analysis and a companion corrective action plan.

Healthcare organizations must strike a balance between enabling patient engagement initiatives and securing patient data.

As healthcare leaders, we must evaluate and manage cybersecurity risks like any other risk and be proactive in protecting our organization. Managing cyber risk is complicated and, to be successful, your entire organization must be engaged.

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

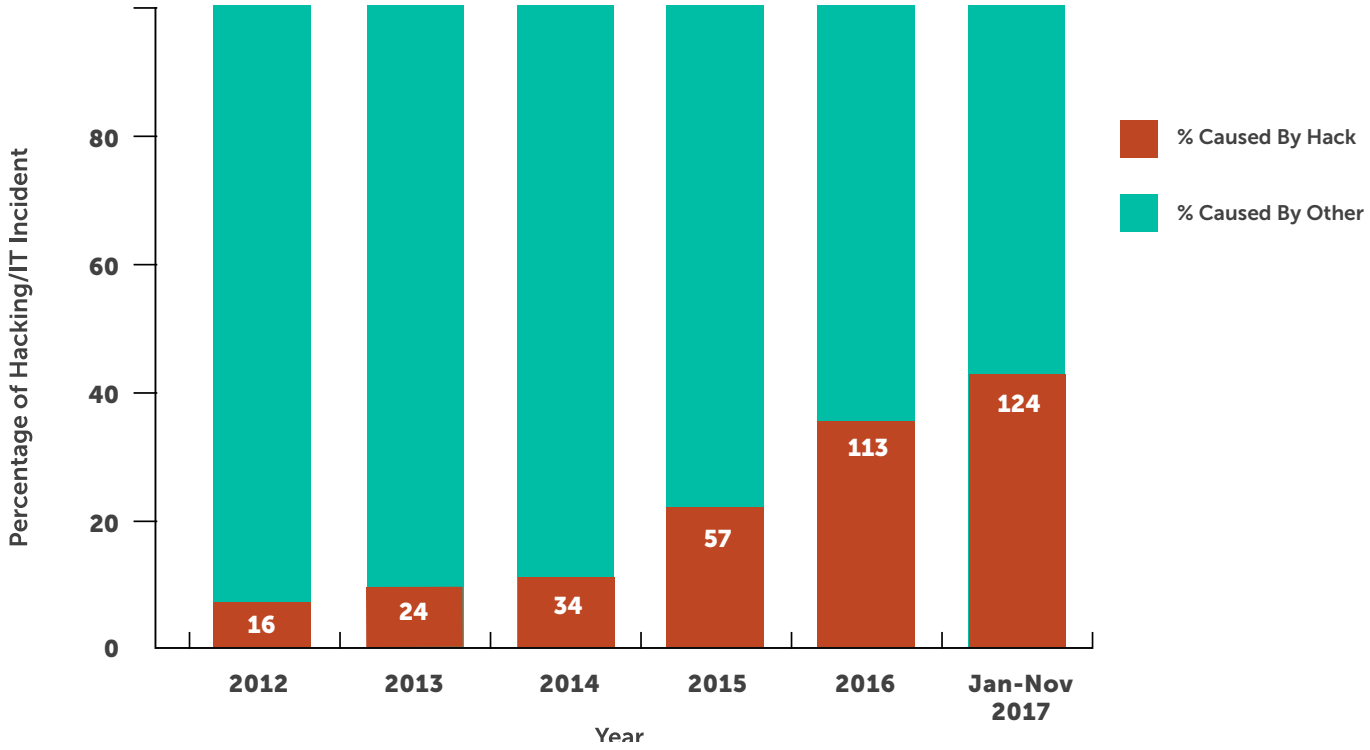
*Source: Top health industry issues of 2016: Thriving in the New Health Economy, PwC Health Research Institute

# 2017 Year in Review

The state of cybersecurity and the frequency of breaches in the healthcare industry intensified in 2017. The number of people directly impacted by a breach decreased year-over-year, but the number of entities impacted increased 25 percent over the last 12 months*. This validates the fear of many healthcare organizations: **hackers have momentum and breaches are happening more often than ever before**. Our adversaries are focused on obtaining valuable health information. In most cases, these breaches are deliberate and directly aimed at obtaining sensitive information for monetary gain. As of mid-November 2017, a total of 303 healthcare entities had experienced a large breach this year. This is on pace to surpass the 327 breaches experienced in 2016. So far this year, over 4.7 million health records have been compromised.

According to data provided by The Office for Civil Rights (OCR), hacking continues to be the biggest cause of breaches for the sixth year in a row. This year, over 40 percent of all breaches were caused by hacking — a 10 percent increase in the number of entities impacted by hacking in 2016. Every year since 2012, when hacking represented only 8 percent of all breaches, it has been a larger cause of breaches than the prior year.

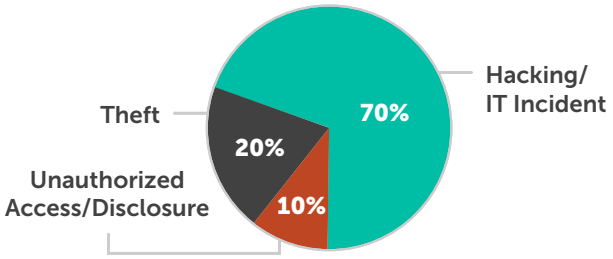
## Healthcare Entities Impacted by Breach




*Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

This data confirms that hacking not only makes up a larger percentage of all breaches, but the number of entities breached by a hack has also increased significantly since 2012. Hacking has also affected the largest number of people thus far in 2017.

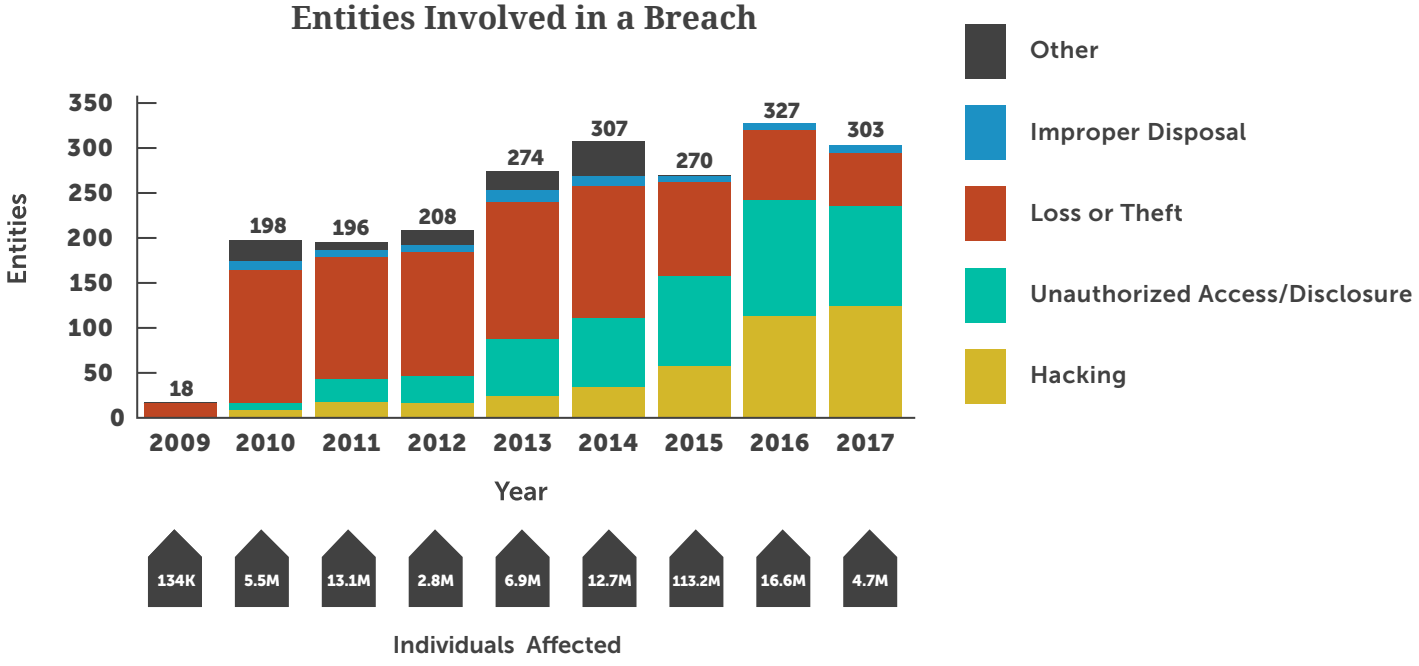
## Percentage of Individuals Affected by Breach Type (January - November 2017)



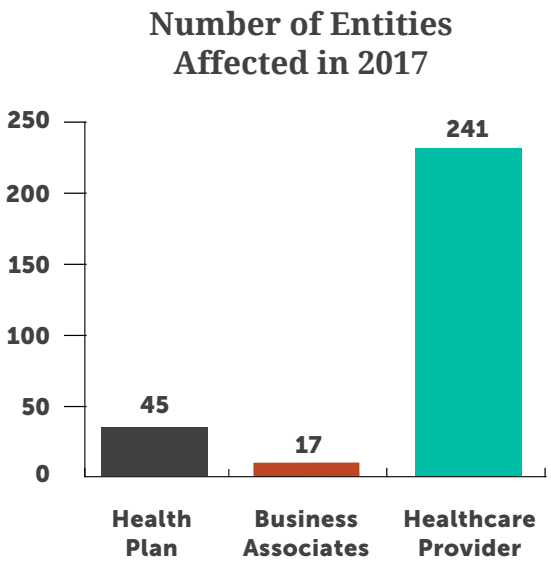

This breach data underscores the importance of a solid security program focused on the fundamentals of patching and employee education. Having a well-executed security program can significantly decrease the chance of a large-scale breach.

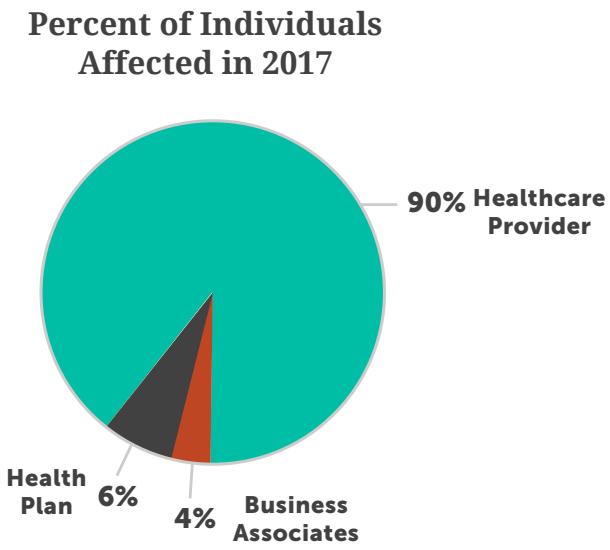
On a positive note, breaches caused by loss or theft decreased for the fourth year in a row. This underscores the progress our industry has made to educate employees on the importance of handling devices that contain Electronic Personal Health Information. It is important to build upon these successes and continue our educational efforts, because phishing continues to be a significant entry point for our adversaries. The best defense against phishing is continuous education and simulated phishing attacks. These activities are fundamental to your security program and are some of the most affordable steps your organization can take.

## Entities Involved in a Breach



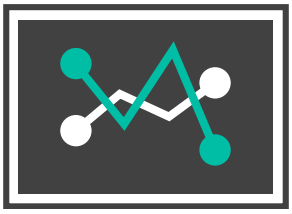
Providers continue to be the most targeted and breached type of healthcare organization in 2017. This has been the case since OCR began collecting breach data in 2009. Providers accounted for 80 percent of all entities breached thus far in 2017 and over 90 percent of all individuals impacted. This is more than health plans and business associates combined. Providers have experienced over 240 breaches this year; we expect that number to climb to over 260 by end of year.




Unlike 2016, there was no single breach in 2017 that impacted over one million individuals. The total of the top five breaches affected over two million people and represented over 43 percent of all those impacted by a breach. Providers accounted for 18 of the 20 largest breaches thus far this year and hacking was the cause of 17 of those 20 breaches. This further emphasizes the focus our adversaries have on the provider segment of healthcare and highlights hacking as their weapon of choice.

| NAME OF COVERED ENTITY | ENTITY TYPE | INDIVIDUALS AFFECTED | CAUSE |
|---|---|---|---|
| Commonwealth Health Corporation | Healthcare Provider | 697,800 | Theft |
| Airway Oxygen, Inc. | Healthcare Provider | 500,000 | Hacking |
| Women's Health Care Group of PA, LLC | Healthcare Provider | 300,000 | Hacking |
| Urology Austin, PLLC | Healthcare Provider | 279,663 | Hacking |
| Pacific Alliance Medical Center | Healthcare Provider | 266,123 | Hacking |



# 2017 Security Risk Analysis Trends

We often speak with clients about how the HIPAA required Security Risk Analysis (SRA) serves as a benchmark to identify and manage organizational risk. A comprehensive SRA can clearly outline and roadmap exactly where an organization should focus its attention and efforts. In 2017, Fortified conducted a security risk analysis, OCR mock audits, HITRUST certifications and strategic security planning for the majority of our clients. Although the clients varied in size, revenue, network complexities and geography, we identified three common trends:

## POLICIES AND PROCEDURES ARE WEAK, OR DON'T ALIGN WITH ACTUAL IMPLEMENTATION OF SAFEGUARDS.

We found that large budgetary purchases or complex software implementations don't always pose a challenge. Instead, the fundamentals of security and risk management are usually missing. Policy and procedures have always been at the heart of a strong security and risk management program. They set the foundation for the organization's rules, guidelines, standards and expectations. Typically, we see organizations fall into one of three groups:

**GROUP ONE**: No policy or procedures are approved and published. This is more common with business associates or newly merged health systems that haven't decided whose policy sets will be the system's adopted set.

**GROUP TWO:** Organizations with approved and published policy sets that aren't being followed. This is particularly dangerous, as senior leaders assume the organization is following the "rules" — yet when you get to the "ground level" it is quite the opposite. Senior leaders possess an unwarranted level of comfort and make decisions on priorities and resources without a clear picture of the organization and its risk.

**GROUP THREE:** Organizations that haven't reviewed and/or updated their policy sets in a number of years. This activity is critical since technology, network environments, leadership, and federal, state and local regulations are always in flux. A sound risk management program will account for all of these types of changes and ensure the policy/procedures reflect those changes.

Regardless of where organizations fall into these groups, having effective policy and procedures should be step one in developing and managing security and risk.

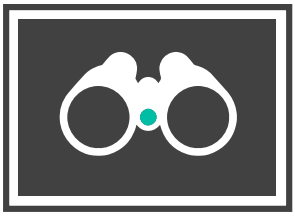
## ORGANIZATIONS LACK CONCISE ASSET INVENTORIES.

The lack of critical asset inventories is another foundational challenge for many healthcare organizations. This year, Fortified has assisted a number of organizations that were being investigated and/or audited by OCR. Throughout that process, organizations have struggled to answer a common question from OCR: "Where is your asset inventory? Specifically, where is the inventory of devices that store, process or transmit ePHI?" Not surprisingly, OCR has a deliberate reason for asking this question. How can you protect ePHI if you don't know where it is? Understanding where your sensitive information resides will help you tailor your controls and safeguards to that specific environment. This type of focused effort can help save time and budgets from being overtaxed.

## LACK OF WELL-STRUCTURED VULNERABILITY MANAGEMENT PROGRAMS.

Organizations must commit themselves to vulnerability management. It is mission-critical to address the real gaps in security that leave sensitive information exposed. In our Mid-Year Horizon Report, we wrote about utilizing a defense strategy around people, process and technology. While each holds its own challenges, in the past 12 months Fortified has seen a number of examples of poor processes, specifically with regard to vulnerability management (Wannacry, Petya, Equifax, etc) that have caused the most issues. There is a seemingly endless onslaught of patches, security updates and fixes to operating systems, applications, databases and networking devices.

While healthcare is concerned with EHR transitions or upgrades, movements to the cloud, or any other IT project, it is imperative that a priority be set on getting back to the fundamentals of risk management and good cybersecurity hygiene. This begins with regular Security Risk Analyses. We must commit ourselves to vulnerability threat management if we want and expect to improve our security posture.



# Penetration Testing Trends: What We've Seen*

Fortified offers and conducts penetration testing for many of our clients. A valuable instructional and educational aid, Fortified engagements allow companies to experience a mock cyber-attack, assess incident response plans and learn how to better secure their overall infrastructure. While each engagement follows a similar process, the penetration test is unique to each client. This is due to such factors as differing infrastructure, internal policies and standard operating procedure. Throughout these penetration tests, Fortified has noticed an alarming trend of identical vulnerabilities among the organizations we test.

**Fortified analyzed penetration tests conducted between 2015 and 2017, which revealed a host of alarming statistics:**

**100%** of web application penetration tests result in demonstrating the ability to access ePHI

**97%** of network/web application penetration tests uncovered critical vulnerabilities

**93%** of network penetration tests demonstrated the ability to gain access to ePHI

**13%** of network/web application penetration tests involve compromise due to SQL injection

**10%** of external network/web application penetration tests result in the discovery of public exposure of sensitive data without authentication

**68%** of external network penetration tests result in breaching the perimeter and gaining full access to the internal network

**72%** of network pen tests result in gaining Domain Admin privileges

**25%** of network pen tests involve compromise due to remote code execution vulnerabilities

**54%** of network pen tests involve compromise due to access control vulnerabilities

**33%** of network pen tests involve compromise due to an insecure Citrix / VMware Horizon / SSL VPN environment

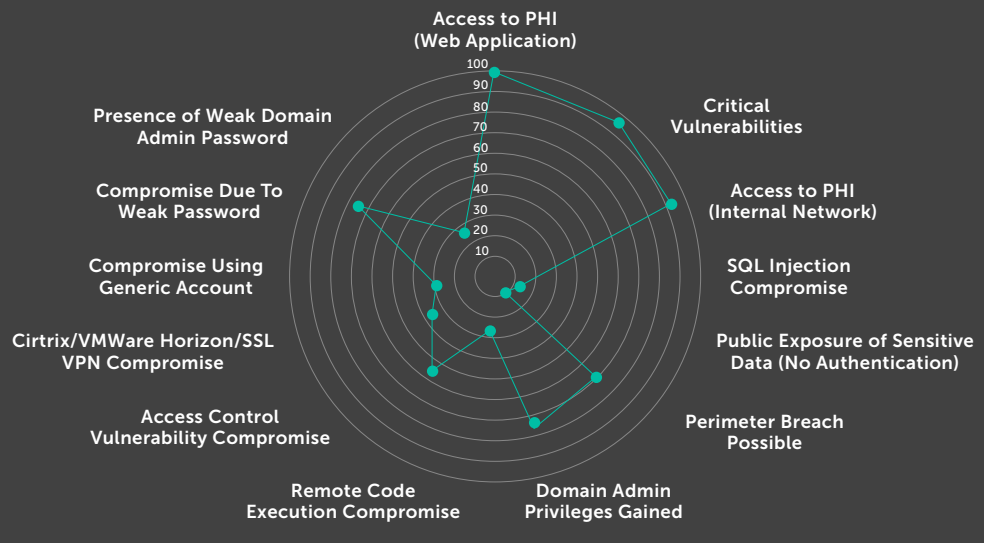
**29%** of network pen tests involve compromise using a generic account (45 CFR 164.312)

**72%** of network pen tests involve compromise due to a weak password

**25%** of network pen tests reveal the presence of a weak Domain Admin password

*This section contains contributions from James Gallagher, Security Analyst at Fortified Health Security.

## Penetration Test Trending Data (Fortified Health Security Engagements)




***FIRST,** healthcare entities are still not understanding the need for strong security engineering when constructing and deploying hardware and software solutions.*

The statistics (and the engagement experience itself) suggest three systemic and continuing issues. First, healthcare entities are still not understanding the need for strong security engineering when constructing and deploying hardware and software solutions. For example, remote access solutions like Citrix and VMWare require extensive knowledge of networking and identity management in order to secure properly. Likewise, secure coding principles must be fully understood prior to constructing a software application that uses a SQL database to store and access PHI. Understanding how a solution impacts the security of an infrastructure is a major step in understanding the overall risk that solution poses. Engineering a secure solution prior to deployment helps to mitigate that risk.

***SECOND,** basic security functions such as strong passwords, password management and patching are being forgotten or totally ignored.*

Second, basic security functions such as strong passwords, password management and patching are being forgotten or totally ignored. Yet, these functions are the foundation for a secure environment and demand constant attention. Strong passwords are a first line of defense for any system and should be enforced without question. Deploying a password management system should include turning off the ability for users to select weak passwords. Applying patches to systems is an operational must and should accompany a regular patch management cycle. Forgetting or completely ignoring such security functions puts healthcare organizations at immediate risk of breach.

***THIRD,** access to PHI is not being configured with "need to know" or least privilege permissions*

Third, access to PHI is not being configured with "need to know" or least privilege permissions. As mandated by HIPAA, PHI must be protected from improper or unauthorized access. The ability for any user to access PHI without prior authorization is in direct violation of HIPAA and puts the organization at serious risk. Consider deploying identity access management systems or even a Data Loss Prevention solution to reduce the exposure to unauthorized users.

# Were We Right? A Look at Fortified's 2017 Predictions

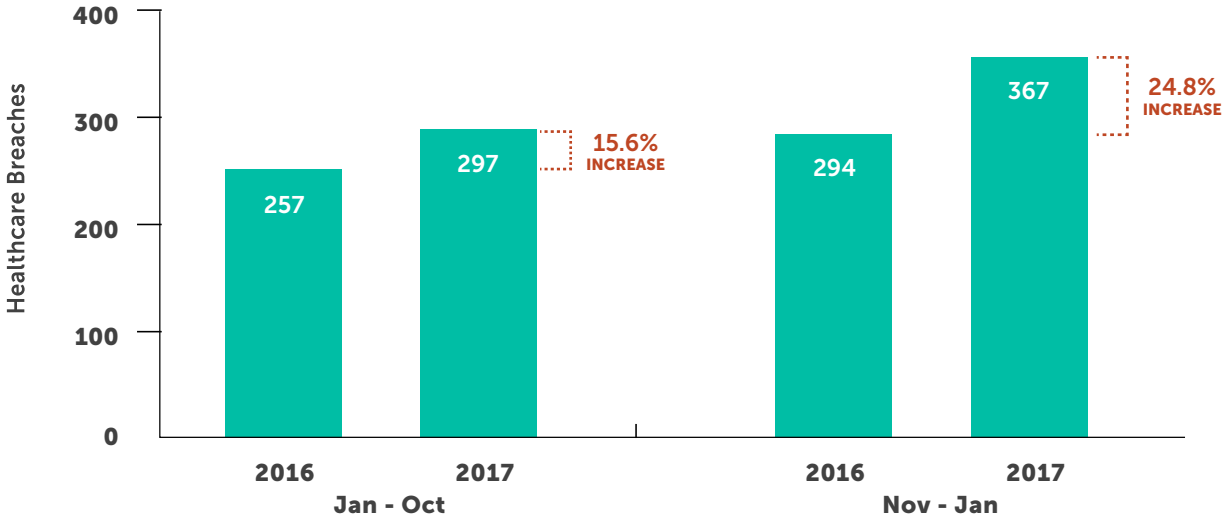
**PREDICTION:**

*Double-Digit Increases in Breach Activity: As hackers become more advanced and better equipped, healthcare organizations will experience a 10-15 percent increase in the number of cybersecurity breaches in 2017.*

## *So how did we do?*

A review of OCR Breach Notification data shows the healthcare industry has seen a 15.6 percent increase in breaches: from 208 in January-October 2016 to 248 for the same time period this year. A 12-month comparison of November 2015-October 2016 to November 2016-October 2017, reveals an even more damaging 24.8 percent increase. As malicious actors continue to assault healthcare organizations, we remain diligent and steadfast in our agenda to improve the security posture of healthcare.

### Healthcare Industry Breaches



**PREDICTION:**

*Boards Will Keep Their Heads in the Sand and Hope for the Best: Some healthcare organization boards have already begun managing cybersecurity risk in the same manner as other business risks. Unfortunately, they often become engaged in cybersecurity risk management after a significant event. Many boards remain content to retain a reactive posture in dealing with cybersecurity concerns. The results will be costly.*

## *So how did we do?*

The double digit increase in breaches bolsters our prediction that boards will remain reactive. We still find CISOs and other security leaders struggling to gain board-level support for the necessary senior management focus and resources required to properly manage and remediate cybersecurity risk. Fortified hasn't changed our perspective or priorities in combatting this very real problem.

**PREDICTION:**

*OCR Moves Towards a National Framework for Healthcare: The Office for Civil Rights will take steps to develop a national framework that is prescriptive in its requirements to guide Covered Entities and Business Associates to the desired end result with regard to protecting sensitive data and ePHI. OCR will finally adopt the HITRUST Alliance's Common Security Framework (CSF) as the national standard or work directly with the National Institute of Standards and Technology (NIST) in developing a new framework that meets the unique needs of the healthcare industry.*

## *So how did we do?*

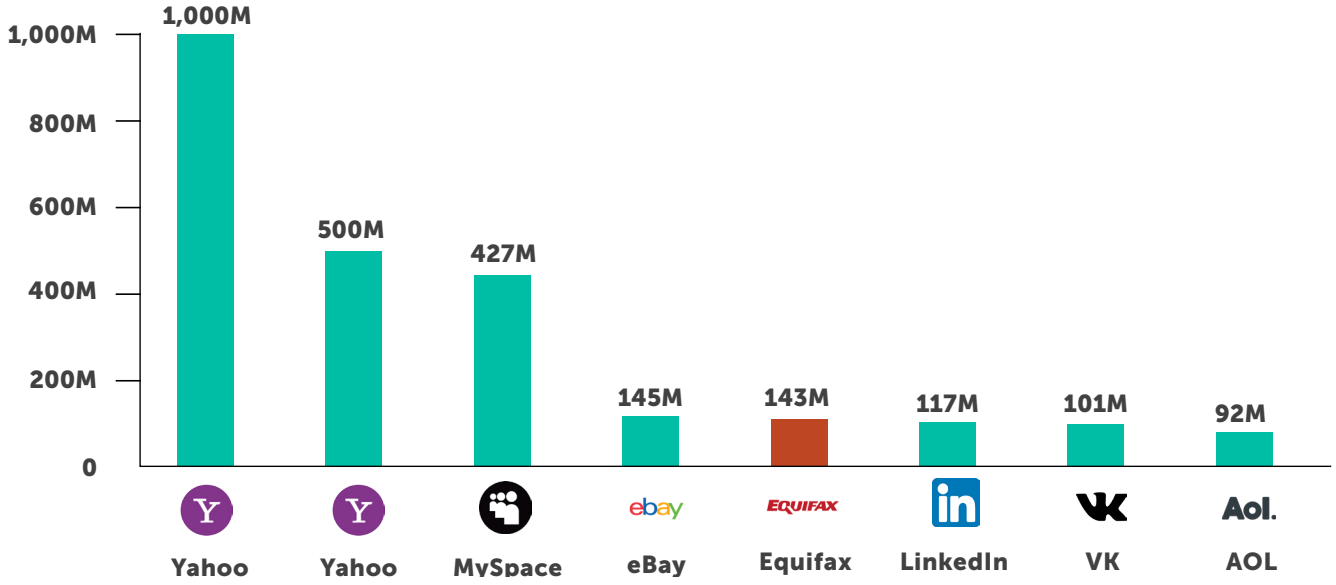
The Healthcare Industry Cybersecurity Task Force has been dissecting the rising issue of healthcare specific threats and impacts for over a year. The Task Force has issued a detailed report containing a number of recommendations, including a call to establish a consistent, consensus-based healthcare-specific cybersecurity framework. The report suggests that a single framework be adopted to unify the industry regardless of entity type. This would provide an easily understood set of standards and lexicon that all healthcare entities can digest and compare. The Task Force cites the federal government's NIST Cybersecurity Framework as an example that could serve as a basis.

*Image Source: Wall Street Journal

# 2017 Equifax Breach: What can Healthcare Learn?

In September 2017, consumer credit reporting agency Equifax experienced a data breach that compromised the personal information of approximately 143 million US consumers (roughly half of the US population). The compromised data included numerous types of personally identifiable information (or PII) including name, birth date, address, credit card number, social security number and driver's license number.

Hackers exploited an unpatched vulnerability in 'Apache Struts', a web application framework in use by Equifax, to ultimately gain access to the now-compromised data.




*Equifax breach in comparison to recent breaches*

Equifax is the financial verification vendor to US Health and Human Services (HHS) for the marketplace exchanges created under the Affordable Care Act. Since much of the compromised data includes PII, this data can be used to steal the health insurance benefits of others, submit fraudulent claims, and receive healthcare services at no cost. This breach has the potential to disrupt healthcare services for some time.

### *What Lessons Can Healthcare Learn from the Equifax Breach?*

1. **Effective vulnerability management is paramount.**

   Although the Apache Struts vulnerability was first announced in March 2017, Equifax did not apply the patches until four months later. Had the patches been applied at the time the vulnerability was discovered, the breach would likely not have occurred.

2. **Timely detection can minimize or completely stop potential data breaches.**

   While not specifically cited as a culprit in the Equifax breach, deployment of security systems such as Data Loss Prevention (DLP), Security Incident Event Monitoring (SIEM) and Intrusion Detection System (IDS) will increase the likelihood of early detection and early response.

3. **Encrypting data ultimately helps protect it.**

   To a malicious actor, the value of stolen data is significantly reduced or eliminated when encryption techniques are applied to data at rest.

4. **Creation of a well-formed incident response plan is key to withstanding any consequences resulting from the Equifax (or any) data breach.**

   Failure to create and implement such a plan can result in loss of consumer confidence, consumer trust, decreased revenue and compliance violations.

   Like previous high profile breaches, the Equifax breach is an educational opportunity for all healthcare organizations. Analyzing and understanding how it happened, the internal incident response actions, and most importantly, how clients respond to this breach can help healthcare organizations avoid or be better prepared for a future breach.

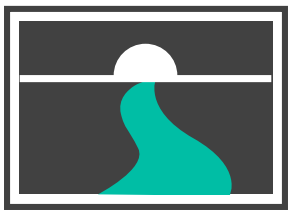
*Sources:

Michael Hiltzik - http://beta.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html

Lily Hay Newman - https://www.wired.com/story/how-to-protect-yourself-from-that-massive-equifax-breach/

Panoptex Technologies - http://panoptex.com/equifax-data-breach-stopped/

Anne Burroughs - https://www.trueprocess.com/equifax-breach-means-healthcare-organizations/



# Looking Ahead

## CYBERSECURITY OUTLOOK 2018

1

**DOUBLE-DIGIT INCREASE IN BREACHES:**
Healthcare will experience a 10-20 percent increase in the number of entities breached, with providers the most targeted and exploited segment.

2

**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.

3

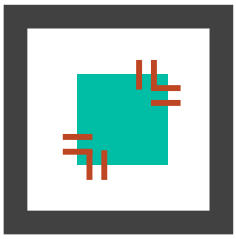
**BREACHES DUE TO BUSINESS ASSOCIATE NEGLECT (THIRD PARTY RISK MANAGEMENT FAILURE) ON THE RISE:**
In 2017, OCR has identified at least 18 breaches due to Business Associate neglect and, more importantly, failure by the covered entity to manage that risk. Healthcare covered entities will continue to experience risk and possible breaches in 2018 unless effective Business Associate risk management programs are established.

4

**INCREASED THREAT TO IOT DEVICES**
Medical devices constitute a large number of IoT (Internet of Things) devices currently attached 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.

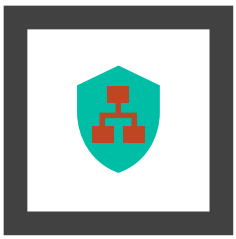
## MOVING FORWARD

- **TREAT SECURITY AS A BUSINESS ISSUE**
  Security can no longer be referred to as an IT problem. The consequences of bad security now reach into every aspect of business. Thus, security should be treated as a business issue and dealt with accordingly. Ensure that sound security decisions are being included at every level of the business.



- **PATCH, PATCH, PATCH**
  Institute a patch management program – Patch your systems. Then patch again. And again. It is a monotonous, somewhat challenging cycle but is extremely important. Much of the malware today is predicated on the vulnerabilities that patching will fix. Establish a patch management program and ensure it is operating properly and often.

- **EXECUTE EXISTING CORRECTIVE ACTION PLANS**
  Corrective Action Plans are designed to help remediate issues within your business. They are also designed to have a finite shelf life. Ensure any Corrective Action Plans you have are actively being worked and have a completion date firmly established. Remediate quickly to avoid a costly breach.



- **SHOW PROGRESS AGAINST COMPLIANCE FRAMEWORKS**
  Healthcare entities are required by law to adhere to HIPAA. But are they truly compliant? Breaches due to HIPAA compliance negligence can result in legal action and hefty fines. Confirm that your organization can clearly demonstrate compliance to HIPAA regulations by having a HIPAA risk analysis performed annually. Ensure any and all Corrective Action Plans resulting from the assessment are fixed in a timely manner.

## 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, Suite 250
Franklin, TN 37067

### ABOUT FORTIFIED HEALTH SECURITY

Fortified Health Security is a leader in information security, HIPAA compliance and managed services, focused 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 partners with healthcare organizations across the continuum, serving health systems, single hospital entities, physician practices, post acute providers, payors and business associates.

*fortifiedhealthsecurity.com*

## ABOUT THE AUTHORS

**Dan L. Dodson** is President of Fortified Health Security where he helps healthcare organizations effectively develop the best path forward for their security program based on their unique needs and current 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), and has held positions with Covenant Health System, The Parker Group, and Hooper Homes. 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 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.

**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.

**Darrin Moran** is the Director of Services at Fortified Health Security where his primary focus is delivering and enhancing the world-class managed services Fortified is known for. Drawing on 20 years of security and IT experience in both government and healthcare industries, his background and education as a Virtual Information Security Officer, coupled with deep technical insights, provide Darrin with the unique capability of being able to effectively translate security issues into business solutions. Darrin currently holds a Master's Degree in Secure Information Systems from George Mason University, a Bachelor's Degree in Computing Engineering from The Ohio State University, is a Certified Information System Security Professional (CISSP) and HealthCare Information Security and Privacy Practitioner (HCISPP).