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

So far, 2016 has proved to be a very challenging environment for healthcare leaders when it comes to safeguarding sensitive patient data. Cybersecurity threats and malicious actors continued to wreak havoc across the spectrum of healthcare organizations. The number of hacking incidents in healthcare has trended upward over the last few years as adversaries have followed opportunity.

It has become blatantly obvious that malicious actors have turned their focus away from the historically lucrative arenas like the financial industry and have been aggressively targeting healthcare data. But why? There are three main drivers:

1. First, **healthcare providers are now digitized**. The 2009 HITECH Act successfully spurred a tidal wave of electronic health record (EHR) implementations which significantly increased the amount of personal health information that is now digital. The speed to implement EHRs nationwide consumed most IT departments' capital budgets and made it almost impossible for healthcare organizations to adequately protect electronic patient data at the same speed as the advancement in their environments. Many organizations now find themselves playing catch-up as it pertains to implementing a security program that addresses the technical and human aspects of protecting patient data.
2. Second, **adversaries now realize that healthcare networks are exploitable** because they tend to be less sophisticated and are easier to compromise.
3. Third, **medical records are reportedly defined as the most rewarding source of personal information** because the information tends to be more complete, encompassing everything from medical insurance numbers to credit card numbers. The market value of medical information is worth 10 times more than credit card data on the black market (1). Due to the comprehensive nature of these records, they can be wielded in many forms from false tax returns to Medicare claims to patient misrepresentations.

The bottom line is that bad actors are more focused on exploiting sensitive healthcare data than ever before. In turn, organizations need to take a depth and breadth approach to managing their cybersecurity posture. This year, the healthcare industry experienced an increase in the number of successful cyber-attacks on providers and a heightened focus on compliance from OCR. Couple this with the prevalence of ransomware, as well as tackling Business Associate risk, many leaders find themselves looking for a silver bullet.

"It's no secret that healthcare is slow to embrace change. That slow pace of innovation means the industry is dangerously behind on understanding and mitigating risk."

With no simple fix to this complex problem, it will take collaboration, investment and a comprehensive, ongoing approach to managing cybersecurity risk organization-wide in order to meet the rising challenge. Managing cyber risk is complicated, but it is most effective when led from the top, well-planned, and supported by data. Be the champion within your own organization and push to elevate the discussion of managing cybersecurity risk.

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,

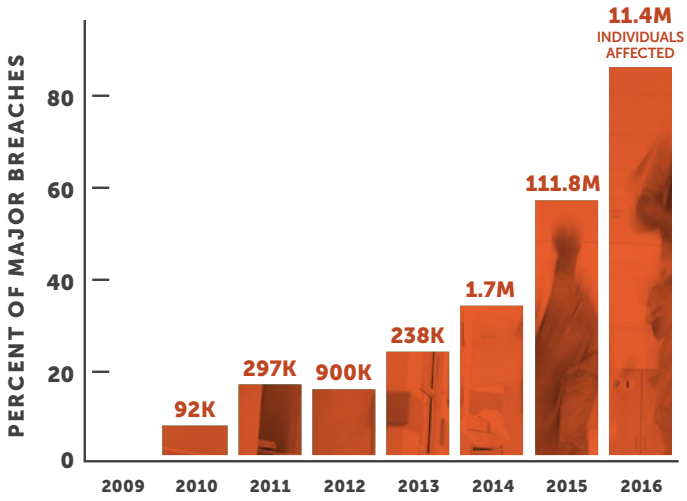
Dan L. Dodson

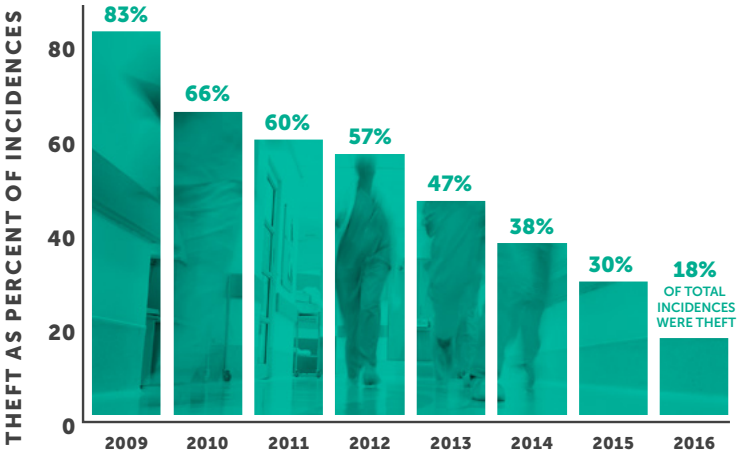
(1) Source: Reuters — http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

2016 Year in Review

While the industry has taken some positive steps as it pertains to safeguarding electronic Personal Health Information (ePHI), our adversaries have matured their tactics, held some of us ransom, and continued to exploit our environments throughout the past year. In just the first 10 months of 2016, the number of entities reporting major breaches caused by hacking has already increased 51% over the full year 2015. This has been a trend since 2012 and will likely continue.

This is according to the "wall of shame" breach data kept by the Office of Civil Rights (OCR) which requires covered entities and business associates to report breaches containing unsecured protected health information affecting 500 or more individuals.





On a positive note, the implementation of cybersecurity educational programs over the past few years by healthcare organizations has increased awareness and led to the reduction in the number of breaches caused by theft. For the third year in a row, the number of entities compromised due to theft has decreased. This year, only 18% of major breaches were caused by theft — down from an all-time high of 83% in 2009.

While this is a step in the right direction, educational efforts for healthcare personnel must be enhanced as ransomware attacks increased in size and scope in 2016. These attacks provide external avenues for hackers to penetrate the network and perimeter defenses of healthcare organizations. In many cases, through phishing, hackers gain credentialed access to the organization's sensitive patient data assets and subsequently encrypt and ransom data for money.

"Many organizations are identifying these potential vulnerabilities and evaluating their exploitability through advanced penetration testing in an effort to enhance their security posture."

Additionally, hackers have access to sophisticated scanning software that allows them to uncover vulnerabilities that may exist in an organization's externally-facing web services. As an example, a simple SQL injection vulnerability found on an organization's website may provide entry — and ultimately access — to the organization's enterprise and patient data assets. Many organizations are identifying these potential vulnerabilities and evaluating their exploitability through advanced penetration testing in an effort to enhance their security posture.

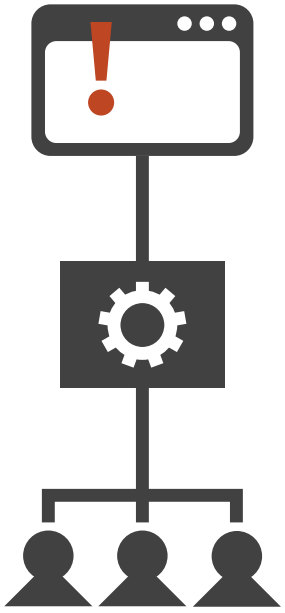
Beyond the increased threat of attacks, there were a number of relevant security issues that manifested themselves in 2016, including:

The increased threat of ransomware

More significant financial settlements with OCR than ever before

A heightened focus on managing third-party risk

Simple vulnerabilities may provide entry — and ultimately access — to the organization's enterprise and patient data assets.



Many organizations are identifying the exploitability of potential vulnerabilities through advanced penetration testing.

The Evolution of Ransomware

The calendar pages of 2016 had just started to turn when ransomware made headlines across the country as hackers held hospital patient information hostage in hopes of big payments. This doesn't represent a new approach to hacking, but the volume and severity of ransomware attacks in healthcare led us to label 2016 "The Year of the Ransom."

THE ORIGINS OF RANSOMWARE

But where did ransomware come from? Most believe that it is a new attack method, but ransomware has a long and storied past. The first known ransomware was the 1989 "AIDS" Trojan (also known as "PC Cyborg") written by Joseph Popp. Basically, victims would receive a floppy disk (remember those?) labeled "AIDS Information Introductory Diskette" and, while booting, the malicious software would hide directories and encrypt the files on the C-drive.

There was a pretty significant lull in activity until 2005 when a new type of ransomware was utilized: Misleading Apps. This malware exaggerated the impact of issues on the computer and required payment to "fix" the issues within the infected system. The evolution continued in 2008 when "Fake Anti-Virus" software was introduced; it would run fake scans claiming to find large numbers of threats and security issues on the computer. In 2011, we began to see "Locker" ransomware which would disable access and control of the computer, effectively locking up the computer from use. Today, we are seeing what most people recognize as ransomware: Crypto-ransomware. This is what we've seen in the news when the malware encrypts local and network file shares and databases.

METHODS OF RESPONDING

The total number of ransomware attacks is largely unknown because many go unreported or only interrupt the functionality of a few devices. However, the potential implication of these attacks are very severe and, in some instances, take heath systems offline for extended periods of time. Without effective controls and a sufficient backup program, you may be forced to pay.

That was the case in February for Hollywood Presbyterian Medical Center when it was forced to pay $17,000 after a ransomware attack took the hospital offline for 10 days. The most unique part of this event was that they went public with the news. This immediately struck fear in the minds of healthcare executives, board members and patients across the country. It was less than a month later when MedStar, a health network of 10 Maryland hospitals, was struck by ransomware and required to move to downtime procedures consisting of paper orders and such while their IT environment was cleansed and restored. This incident reportedly forced MedStar to turn away patients and send them to neighboring facilities. The difference here is that MedStar did not pay the ransom but leveraged backups to restore their systems.

"Without effective controls and a sufficient backup program, you may be forced to pay."

These two events played out in the public media but there are many other examples that didn't hit headlines. Ransomware represents enormous risk to healthcare organizations because operations and patient care can be greatly impacted. This led the HHS Office for Civil Rights (OCR) to provide additional guidance in July of 2016. Specifically, OCR brought clarity to the question often asked by many Covered Entities and Business Associates: "If our organization is hit with ransomware, is the event considered a breach under HIPAA Rules?" (2) (3) OCR's guidance is that a fact-specific determination must be made but, unless the CE or BA can demonstrate there is a "low probability that PHI has been compromised," a breach of PHI is presumed to have occurred. In this event, the entity must comply with current breach notification protocols. This clarification by OCR was significant as it will likely prove to be difficult for most healthcare organizations to demonstrate "low probability" in the event they are breached via ransomware.

BEST PRACTICES

There are number of best practices that your organization should consider as it pertains to ransomware. The first step is for your entire organization to understand that this is more than an IT problem, so your plan must encompass every employee at your organization. The bottom line is Defense in Depth. The best prevention is taking proactive security measures around people, process and technology.

"The best prevention is taking proactive security measures around people, process and technology."

As the greatest risk to an organization, the people aspect must be strictly focused on through an engaging and continuous security and awareness training program. The program should be metrics-based to ensure the program's effectiveness can be measured and managed to drive results. Conducting regular phishing exercises is a cost effective way to measure the success of your program.

As for process, every organization should create and test an effective disaster recovery, business continuity, incident response and breach notification program. Remember: Backups, Backups, Backups! The key here is to test these programs and plans proactively. The first time cross-functional teams meet should not be directly after the attack when it is time to act quickly. We have found that tabletop exercises are an effective method for testing the completeness of

RANSOMWARE BEST PRACTICES:

- Address ransomware across the entire organization
- Implement proactive security measures around People, Process and Technology
- Develop a metrics-based awareness training program
- Create and test a disaster recovery, business continuity, incident response and breach notification program
- Backups, backups, backups!
- Don't under-invest in managing technical point solutions

Sources

(1) http://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html

(2) http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

these programs. Additionally, organizations should perform regular penetration testing, vulnerability assessments and maintain a comprehensive patch management program.

"Simply put: buying technology is half the journey; don't under-invest in managing your technical point solutions over time."

To complete the depth and breadth approach, multiple technologies should be considered including Security Information & Event Monitoring (SIEM), Intrusion Prevention System/Intrusion Detection System, SPAM/Email Filters, Web Content Filters, Anti-Virus/Anti-Malware, NextGen Firewalls, Data Loss Prevention (DLP) and Vulnerability Scanning. Remember that many of these advanced technical solutions will require a level of expertise within your IT department, as many require configurations, monitoring, and ongoing management. You may end up disappointed if you don't adequately support these technical solutions because your perceived value will end up much higher than the actual value to your security posture post-implementation. Simply put: buying technology is half the journey; don't under-invest in managing your technical point solutions over time.

OCR Update

The Office for Civil Rights (OCR) made three major moves in 2016 that affected healthcare organizations significantly, which included launching new audit protocol, levying the most settlements ever, and increasing focus on Business Associates.

1. Launched New Audit Protocol

First, OCR began round two of their audit protocol in 2016 which expands their scope to include Business Associates (BAs) along with Covered Entities (CEs). As part of the program, OCR announced that it would dedicate more resources to investigate breaches of 500 records or fewer. Although in steep contrast to their previous work plan, OCR has, at times, investigated these types of breaches but only in unique cases and as resources permitted. This new direction is to encourage covered entities to take action addressing non-compliance with the HIPAA Security and Privacy Rules regardless of the size of the breach.

OCR has already levied fines against organizations with a breach of fewer than 500 records. In June of 2016, the Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) agreed to pay $650,000 in fines after a CHCS portable device with 412 patient records was stolen. A more sizable settlement was levied against the Triple-S Management Corporation in November of 2015. Triple-S has agreed to settle potential violations of the HIPAA Privacy and Security Rules in the sum of $3.5 million. OCR initiated investigations after receiving multiple breach notifications from Triple-S involving unsecured protected health information (PHI).

2. Levied Unprecedented Number of Settlements

Second, OCR has made more HIPAA violation settlements thus far in 2016 than any other year since 2009, totaling more financial penalties than the last four years combined. So far in 2016, 12 organizations have been penalized over $22.8 million dollars for HIPAA violations by the Office of Civil Rights (OCR). This is double the number of settlements reached in 2015 and a 268% increase in financial penalties over last year. This includes the largest settlement ever of $5.5 million whereby Advocate Health System agreed to a settle HIPAA violation claims related to three data breaches that occurred in 2013. We expect the level of oversight and severity of penalties to continue to rise over the next few years. Confirming this notion, OCR has stepped up their audit program and levied fines for smaller breaches.

3. Increased Focus on Business Associates

Third, the lines of responsibility between Covered Entities (CE) and Business Associates (BA) continue to blur in the eyes of OCR. Or, at a minimum, if CEs don't manage BA risk appropriately, they may face financial penalties in the event that their data is breached at one of their BAs. In March of 2016, there was a major settlement between OCR and North Memorial Health Care because they failed to implement a Business Associate Agreement with a major contractor. Furthermore, they failed to institute an organization-wide risk analysis program to address risks and vulnerabilities to protect patient information. This marked the first major incident whereby a covered entity faced significant financial penalties along with significant remediation requirements because of the actions of a business associate. A laptop was stolen from the car of a North Memorial Health Care BA employee's car which contained 289,904 patient records and, due to their current business associate management process, they were forced to settle with OCR. This underscores the importance of business associate management. This risk is intensifying as Business Associates were responsible for 25% of the total number of individuals impacted by a reported breach year to date. Financial penalties coupled with the increase in attacks on BAs is a compelling reason for healthcare organizations to formally assess, audit and manage them more comprehensively. Business associate management is a critical element of any robust cybersecurity management program and will likely garner more attention in the coming years.

"As healthcare leaders, we must balance fighting these adversaries through advanced technical solutions with educating our employee populations about cyber responsibility — all while maintaining an already strapped IT budget."

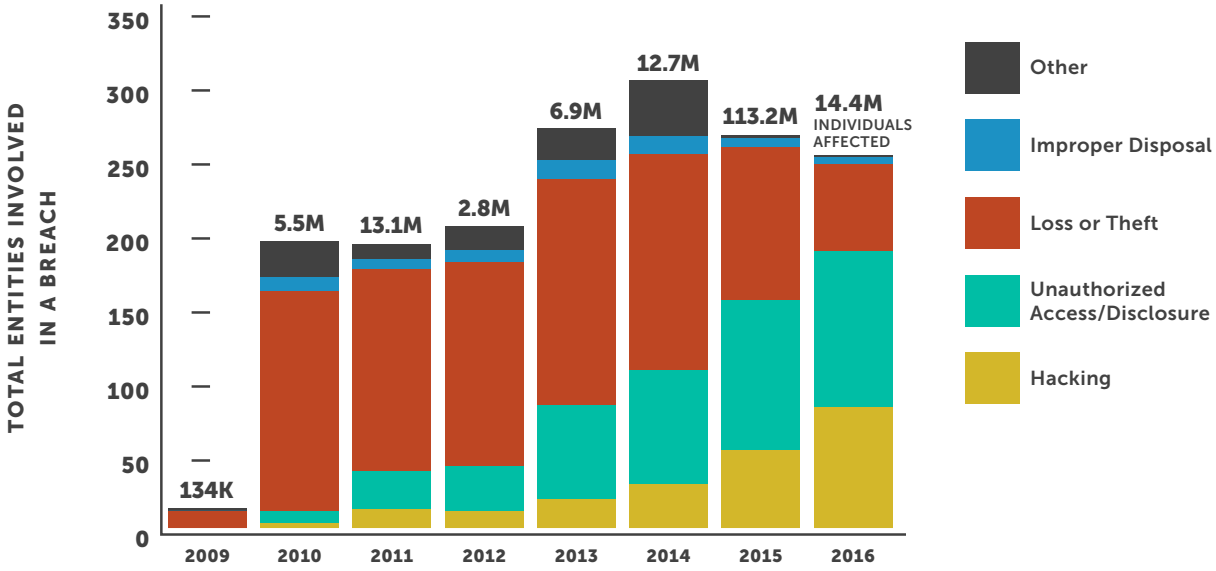
It will come as no surprise to you that 2016 marked another year of vicious attacks. As healthcare leaders, we must balance fighting these adversaries through advanced technical solutions with educating our employee populations about cyber responsibility — all while maintaining an already strapped IT budget. The first step in building a successful cybersecurity risk management program is to elevate the discussion beyond IT to include every facet of the organization including the hospital board. The most successful organizations leverage data to drive these discussions, build the right case and demonstrate the importance of cyber risk. This often starts with an understanding of the overall significance of the threats facing your organization and analyzing the breach data which we will break down in the next section.

2016 Breach Data Review

The state of cybersecurity and the anatomy of a breach in the healthcare industry has changed.

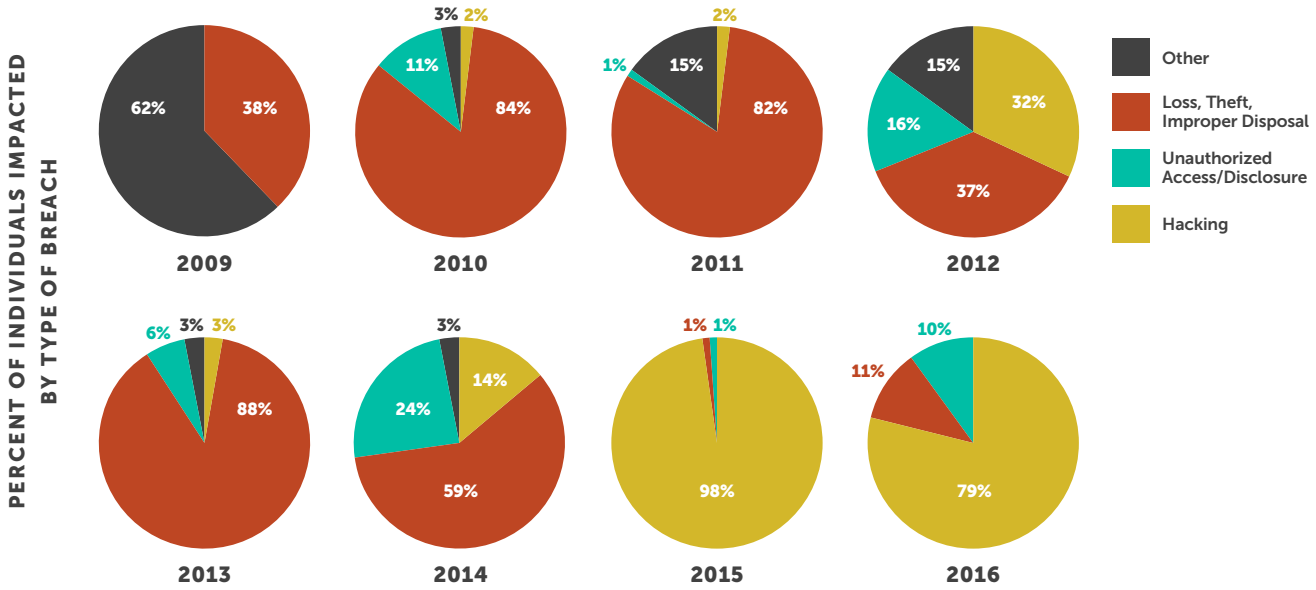
Long gone are days when the primary driver of breaches was an employee mistakenly sending a file with hundreds or thousands of patient records to their personal email, or a laptop being stolen out of the back of a car. The landscape has changed. The industry has changed. The disclosure vectors have changed and the outlook is much more direct and detrimental. Breaches are deliberate and calculated. As of October 2016, a total of 256 entities had experienced a large breach this year, which is on pace to surpass the 270 breaches experienced in 2015. **So far, a total of 14,401,029 patient health records have been compromised.**

According to the OCR breach data, the number of entities that experienced a Hacking or Unauthorized Disclosure incident has trended upwards 406% and 304% respectively since 2011. Theft or loss as the cause of breach has trended downwards significantly with a decrease of 57% during the same time period.



This data validates that, although awareness has risen, which has reduced theft or loss, the overall industry still has significant exposure to potential breaches.

Healthcare has been targeted and breached more in the last two years than it is has since OCR began reporting data in 2009. This is alarming because our industry has been slow to implement industry-leading security technologies and effectively engage staff as well as senior management. We are now seeing the fallout of years of neglect — but there is light at the end of the tunnel. Historically, the majority of breaches were the result of inadvertent user error, whereas today we see the opposite. Loss, Theft or Improper Disposal represents 11% of all impacted individuals in 2016, down from an all-time high of 84% in 2010.



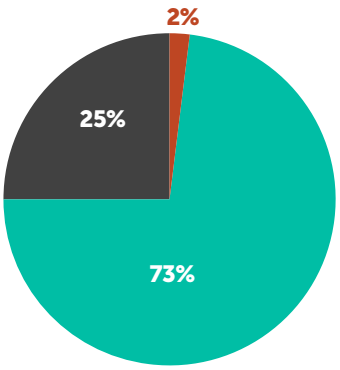
The healthcare industry has done an impressive job improving its employee training to address the controllable human element of employees not understanding the impacts of mishandling or negligent handling of ePHI. The problem has now become a matter of lack of security tools, technologies and technical controls to combat the constant barrage of attacks and social engineering attempts.

"Employees need to understand that their actions — even when not handling sensitive information — can result in a breach."

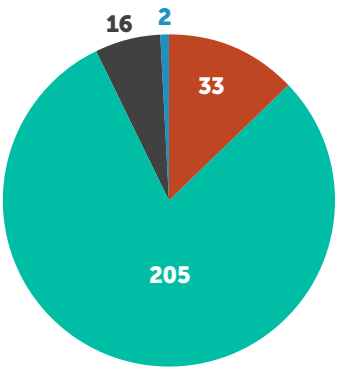
Healthcare organizations need to augment their normal security training that covers proper handling of ePHI to also address the nuisances of phishing, vishing and ransomware. Employees need to understand that their actions — even when not handling sensitive information — can result in a breach. Healthcare organizations need to deploy a constant and engaging cybersecurity educational process in order to keep security and proper computing hygiene at the forefront of each employee's mind.

Healthcare providers are by far the most targeted and attacked type of healthcare entity. This is not new. Healthcare providers have experienced the highest number of breaches every year since 2009. Furthermore, we have seen increases in the number of provider organizations compromised year-over-year since 2014. In 2016, healthcare providers represented the vast majority of entities involved in a breach and affected more individuals than health plans, clearing houses and business associates combined. Almost three-fourths (73%) of individuals affected this year were exposed by a provider organization breach. Providers have experienced 205 breaches to date, representing an increase of 6% over the full year 2015. This percentage increase will likely grow by year end.

"Healthcare providers have experienced the highest number of breaches every year since 2009."



PERCENT OF INDIVIDUALS AFFECTED IN 2016



NUMBER OF ENTITIES AFFECTED IN 2016

Business Associates breaches impacted 25% of the total number of individuals affected by a major breach. This is an increase from 3% in 2015 and represents a total of 16 business associates breached thus far this year. Health Plans experienced a decrease in the number of entities involved in 2016 from 62 in 2015 to 33. Given the size of the 2015 Anthem, Premera Blue Cross and Excellus breaches, with 99,800,000 patients impacted in total, Health Plans have impacted a significantly smaller number of people thus far in 2016 as compared to 2015.

One trend that continued in 2016 is that a few incidences impacted the majority of individuals affected this year. For instance, 75% of records breached YTD (10,834,278) came as a result of the Top 5 breaches.

NAME OF COVERED ENTITY	ENTITY TYPE	INDIVIDUALS AFFECTED
Banner Health	Healthcare Provider	3,620,000
Newkirk Products, Inc.	Healthcare Provider	3,466,120
21st Century Oncology	Healthcare Provider	2,213,597
Valley Anesthesiology and Pain Consultants	Healthcare Provider	882,590
Bon Secours Health System Incorporated	Healthcare Provider	651,971

CYBERSECURITY INSURANCE CLAIMS DENIED

Last year, the first major breach occurred where a cybersecurity insurance company required a health system — which had an in force insurance policy at the time of an attack — to payback their insurance claim after it was determined that their underwriting application did not accurately represent their security controls. Although these events unfolded very publicly in 2015, this is a very important lesson and relevant for all healthcare organizations, as many organizations took steps in 2016 to incorporate cybersecurity insurance as part of their overall cybersecurity program.

Purchasing cybersecurity insurance requires expert scrutiny as contracts are not standardized. Organizations should be careful when evaluating and selecting cyber insurance. This is certainly an area where seeking the advice of a professional insurance broker or security expert may prove to be useful. Furthermore, the criteria that your organization commits to as part of the application process must be embedded into your ongoing security management program to help ensure compliance with the policy.

Cybersecurity 2017 Outlook

Many entities will evolve next year while others will continue to deprioritize cybersecurity. This is a mistake, given what is on the horizon for next year. We predict healthcare organizations can expect the following next year:

- **Double-Digit Increase in Breaches:** As hackers become more advanced and better equipped, healthcare organizations will experience a 10-15% increase in the number of cybersecurity breaches in 2017. Ransomware attacks will increase.
- **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. With that said, we predict that many Boards will be content to retain a reactive posture in dealing with cybersecurity concerns. The results will be costly.
- **Increase in Civil Litigation:** Significant pressure from civil litigation, due to the breach of ePHI, using federal regulations, HIPAA/HITECH, as a standard of due care will be seen in 2017. Healthcare and cybersecurity are massive economic growth sectors, drawing the attention of both consumers and attorneys as litigation targets. As consumers have become more regulation-savvy and the legal lay of the land is better understood by attorneys, opportunities to file complaints will be seen exponentially increased over past years.
- **Budgets Won't Be Big Enough:** Given the threat landscape, we believe that most healthcare organizations will outspend their 2017 cybersecurity budgets by over 50%. Most organizations budget too little on cybersecurity and then experience overruns in an attempt to respond to emerging threats.
- **OCR Moves Towards a National Framework for Healthcare:** The Office for Civil Rights will take steps to develop a national framework specific to the healthcare industry that is prescriptive in its requirements in order to guide CE and BA to the desired end result with regards to protecting sensitive data and ePHI. We feel that the OCR will finally adopt the HITRUST Alliance's Common Security Framework (CSF) as the national standard or work directly the National Institute of Standards and Technology (NIST) in developing a new framework that meets the unique needs of the healthcare industry.

It is time for healthcare to work to outpace cybersecurity threats. A proactive posture is a critical strategic investment. It is imperative that healthcare leaders realize that solving these problems will take the focus and strength of their entire organization. Much like long-term business goals and objectives, healthcare leaders need to develop strategic security roadmaps that will improve their posture over time.

"It is imperative that healthcare leaders realize that solving these problems will take the focus and strength of their entire organization."

Moving Forward

So where do we go from here? Here is a list of six things you can do to increase your cybersecurity profile starting now:

- **EDUCATE THE BOARD**
  Security begins and ends with executive buy-in. Invest time in making sure Boards are informed and involved in order to ensure that the appropriate resources are allocated to cybersecurity.

- **ENGAGE THE WHOLE ORGANIZATION**
  Security is NOT an IT problem; it takes a village. Risk decreases as more people throughout the organization are empowered to identify and respond to threats.

- **CORRECTIVE ACTION PLANNING**
  Develop and execute corrective action planning in order to remove vulnerabilities and improve overall cybersecurity posture.

- **MAKE SURE YOUR TECHNOLOGIES ARE WORKING IN CONCERT**
  Be sure to leverage your investments in a comprehensive and collaborative manner that improves your efficiency and effectiveness. Make them work for you.

- **BE COMPLIANT WITH CYBER INSURANCE REQUIREMENTS**
  Do not think of cyber insurance as a safety blanket. Active compliance with contractual requirements is key to a strong cybersecurity posture.

- **SEEK OBJECTIVE OUTSIDE PERSPECTIVES**
  While a strong cybersecurity posture takes a village, consider input from experts outside your organization in order to contribute new perspectives on your efforts.

We hope this 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, 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.*