The Report Committee for Daniel F Rueda
Certifies that this is the approved version of the following Report:

Healthcare Is The Most Breached Industry, How Do We Change That?

APPROVED BY
SUPERVISING COMMITTEE:

Kenneth Fleischmann, Supervisor

Craig Blaha

Healthcare Is The Most Breached Industry, How Do We Change That?

by

Daniel F Rueda

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Identity Management and Security

The University of Texas at Austin

December, 2017

Abstract

Healthcare Is The Most Breached Industry, How Do We Change That?

Daniel F Rueda, MSIMS

The University of Texas at Austin, 2017

Supervisor: Kenneth Fleishmann

Healthcare is the most breached industry in the United States. Health records are now fetching more money on the black market than credit card numbers. Threats to Healthcare data security come from criminal hackers, hacktivists, state-sponsored hackers, malicious employees with perhaps the greatest threat coming from accidental or negligent disclosure by employees. Most information security related investments are driven by the need to meet Health Insurance Portability and Accountability Act (HIPAA) requirements. Typically, these investments are characterized by heavy reliance on technology, outsourcing security activities, and risk transfer (Cyber Liability Policy). As a result of this compliance focused security spending, little headway is made in reducing the number of breaches in healthcare. Two important weaknesses that will continue to inhibit progress in protecting health information are: the industry lacks a culture of security, and there is a lack of strong leadership among those tasked with overseeing information security.

Table of Contents

List of Figures

Introduction

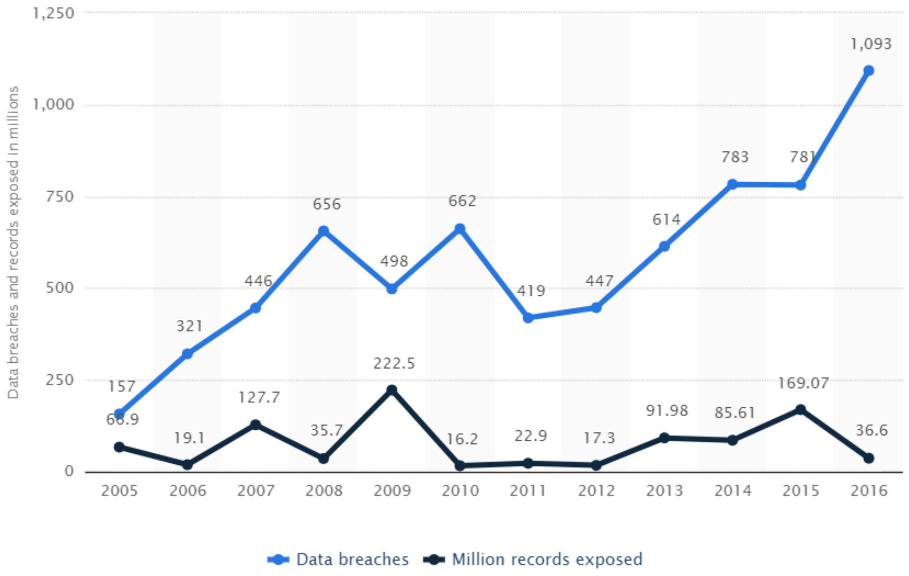
Hacking has become an almost ubiquitous phenomenon in recent times, in 2016 U.S. industries endured 1,093 data breaches.(Karif 2017) Although we tend to think of hacking as a modern phenomenon, many believe the first electronic hack took place in 1903, long before computing. Italian inventor and engineer Guglielmo Marconi was a pioneering figure in the field of wireless telegraphy. Marconi demonstrated the ability to wirelessly transmit Morris Code as early as 1896, the technology advanced so quickly that Marconi made his first transatlantic transmission in 1901. Marconi's technical advancement of the science of telegraphy also set him up to be an early commercial pillar in the industry, Marconi proved to be a skilled businessman. An early concern regarding the transmission of wireless messages, not surprisingly, revolved around privacy. To address this concern, Marconi pledged in a 1903 issue of St James Gazette (Gascueña, 2016), to deliver messages over confidential channels. Marconi claimed that he could tune his receiver and transmitter in a way that would ensure transmissions would not be intercepted. Marconi set about to demonstrate his ability to confidentially transmit wireless messages during a lecture session at the Royal Institution in 1903. During this session, a colleague of Marconi, named John Ambrose Fleming would receive a message transmitted by Marconi from his Laboratory in Cornwall England. The demonstration did not go as planned.

Neville Maskelyne was a British magician, who also had an interest in telegraphy. He was commissioned by the Eastern Telegraph Company to see if he could disprove Marconi's ability to send confidential messages. Maskelyne started by setting up a 50-foot antenna mast to see if he could intercept messages that Marconi was already sending to ships off the English coast. He discovered that with relative ease and without tuned receivers, he could easily intercept the signals without anyone becoming aware.

During the conference at the Royal Institution, John Fleming was preparing his receiver for the demonstration when it suddenly began to tap out a message in Morse Code. To all in the audience, it sounded like normal code, but Fleming knew that something was amiss. The First message repeated the words ‘Rats, Rats, Rats’. Then it changed to a sort of poem, "there was a young fellow of Italy, who diddled the public quiet prettily….” And so on. The rogue messages stopped just before Marconi’s messages arrived; Fleming called the act “scientific vandalism” (Gascueña, 2016) in a letter to The Times a few days later. Maskelyne sought to embarrass and discredit Marconi, he thought of it as nothing more than a prank, but the act has gone down in the annals of history as what many believe to be the world’s first act of hacking.

Breaches in the 21st

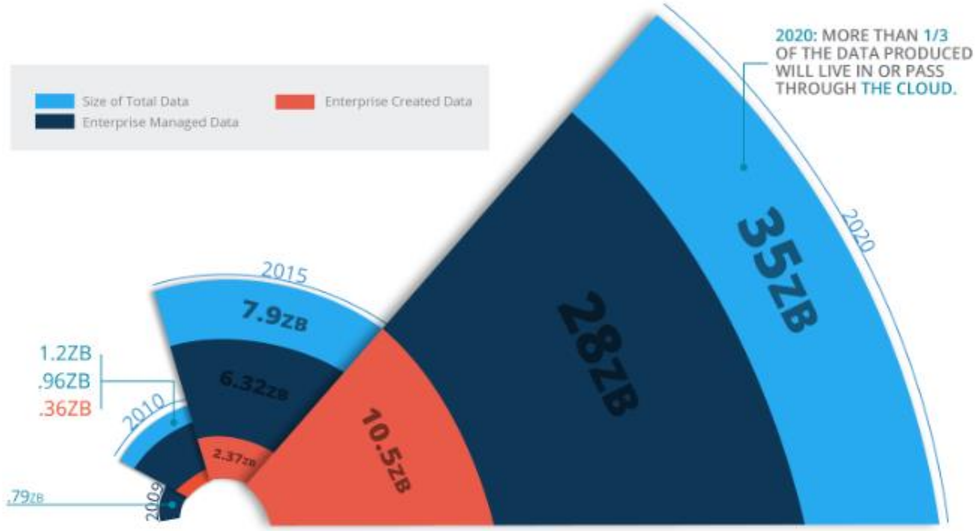
Fast forward to the 21st century, data breaches have become almost ubiquitous as nearly every industry has become increasingly reliant on digital data, cloud computing, and mobile working. The sheer volume of data being stored by companies continues to grow, and the storage of this data increasingly becomes more geographically distributed. Data is stored on workstations, local servers, backup media, in the cloud servers, and data is stored on enterprise or distributed databases. As the landscape of data storage gets more complex, the process of breaching this data is still often still as simple as gaining access to a restricted network by using legitimate account credentials obtained illegitimately. As breaches became more commonplace throughout the 1990s and 2000s, so did the public's awareness and concern for the implications of their private information being breached. According to the privacy rights clearinghouse, since 2005 approximately 1,073,490,127 Records have been breached as a result of roughly 7,800 reported data breaches. Indeed, many Americans are counted twice in that number, but with a number that high, it's safe to say that nearly every single American has had there PII, caught up in a data breach.



© Statista 2017

https://www.linkedin.com/pulse/cybersecurity-youre-paranoid-everyones-out-get-

Figure 1



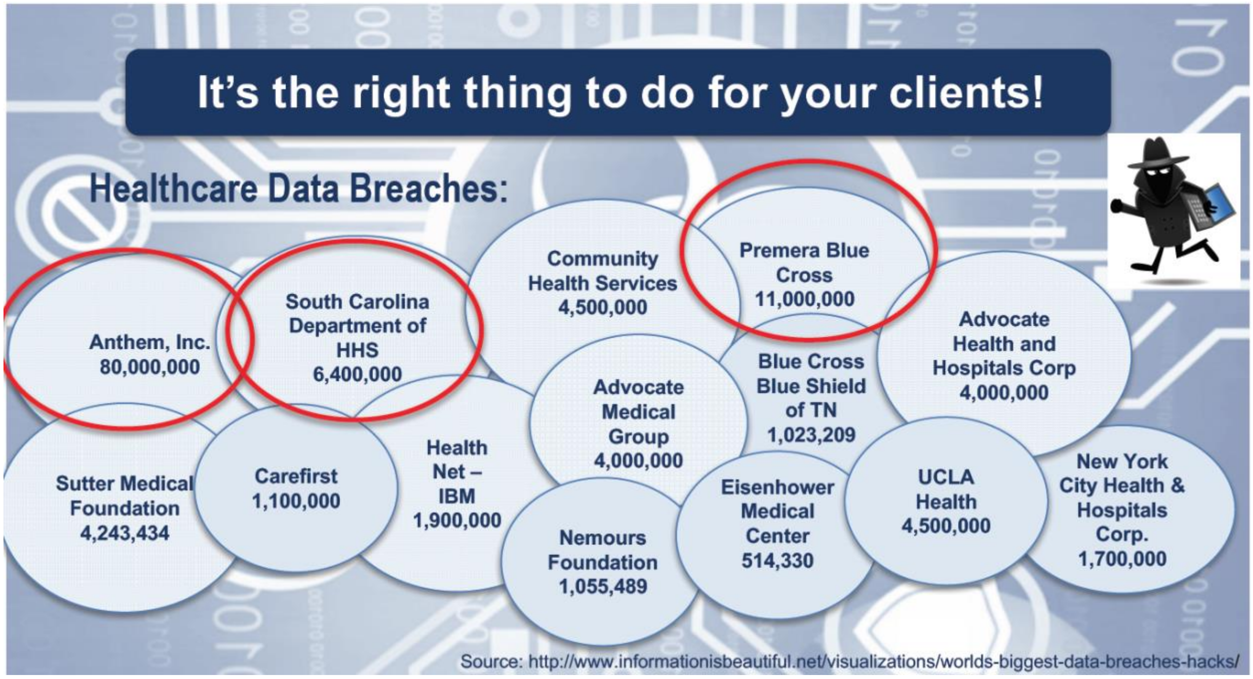
https://www.linkedin.com/pulse/rapid-growth-global-data-hosneyara-begum/

Figure 2

In recent years hackers and cybercriminals have shifted their focus from banks and finical institutions to healthcare institutions, in 2015 alone, over 100 million healthcare records were compromised. (Munro 2016) Part of the shift due in large to the fact that health records are now worth more than credit card numbers, by in large due to the increasing popularity of health insurance fraud. Health records are also useful in other identity type crimes because the amount of personally identifiable information (PII) typically contained. Combine those two factors with the industry’s immature security practices, relative to the financial industry, and it's not hard to understand why healthcare has had such large breaches (see figure 3).

In December of 2014, a database owned by Anthem, the nation’s 2nd largest insurance provider was compromised, as a result early 80 million recorded were breached (Brook, 2017). The attackers, in this crime, were sophisticated, although the hack itself may not have been. As many as five information technology employees had their credentials compromised, which gave the attackers the access they needed to extract the records.

The attackers initially gained remote access, via a low-tech phishing email, then were able to move laterally across the Anthem systems as they continued to escalate privileges by obtaining additional credentials. The hackers utilized as many as 50 stolen accounts covering nearly a hundred systems. Finally, the hackers made their way into Anthem’s enterprise data warehouse system. The warehouse contained millions of records which the hackers were able to exfiltrate successfully. This info included names, birth dates, Social Security numbers, home addresses and other personal information. Anthem spent millions of dollars on the investigation, notification of affected individuals, remediation, attorneys, lawsuits, fines and credit monitoring service. (McGee, 2017) The source has not been officially identified but has been attributed by multiple sources to a nation state-affiliated group, most likely the Chinese. (McGee, 2017)



It's the right thing to do for your clients!

Healthcare Data Breaches:

Anthem, Inc. 80,000,000

South Carolina Department of HHS 6,400,000

Community Health Services 4,500,000

Premera Blue Cross 11,000,000

Advocate Health and Hospitals Corp 4,000,000

Advocate Medical Group 4,000,000

Blue Cross Blue Shield of TN 1,023,209

Sutter Medical Foundation 4,243,434

Carefirst 1,100,000

Health Net – IBM 1,900,000

Nemours Foundation 1,055,489

Eisenhower Medical Center 514,330

UCLA Health 4,500,000

New York City Health & Hospitals Corp. 1,700,000

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Figure 3

In 2011 Sutter Health, a California based system with over 20 hospitals, suffered a massive breach affecting approximately 943,000 patients. Unlike, the anthem breach, a stolen laptop was to blame; the computer was taken from a Sutter Office park in Sacramento. Unfortunately for Sutter, the organization was in the process of encrypting all hard drives on desktops and laptops and was nearly complete with the project. Unfortunately, the stolen laptop had yet to be encrypted. Had it been, Sutter would have protected under the HIPAA safe harbor provisions. The device did not contain any medical records but did contain a database which included names, addresses, DOBs, phone numbers, email addresses and medical record numbers of Sutter Patients.

In another breach, one of the largest healthcare-related breaches, Community Health Systems lost over 4.5 million records. The Tennessee based hospital group owns or operates over 200 hospitals in 29 states, the information lost included patient names, addresses, birthdates, telephone numbers, and social security numbers. Although Community Health's official explanation of the incident suggest that the attack was highly technical and conducted by skilled criminal hackers, a number insiders suggest the hack was significantly less technical. It appears the hackers gained access to the network via a test server that should not have been connected to the internet at all. Because the test server was not supposed to be connected to the internet, a number of security features that should have been deployed were not installed. Because the server was live, the hackers were able to gain access to it via a Heartbleed bug. Unfortunately for Community Health, sensitive VPN credentials were stored on the server, the hackers subsequently used the credential gain remote access to Community Health's system and extracted millions of personal records. It was as though CHS left the lights on and a note on the door, saying, "Hey, come on in, The key is under the doormat!". (Knippa, 2014)

Nowadays breaches seemingly occur on a daily basis and although complacency may not have played a role in the Community Health Breach, complacency among those responsible for enterprise cybersecurity has to be a major concern. I loathe the John T. Chambers quote "There are two types of companies: those that have been hacked, and those who don't know they have been hacked." Although there is undoubtedly some truth to the statement, acceptance of it as fact practically begs that those responsible for cybersecurity will become resigned to the idea of the inevitability of a data breach. Those leaders will act accordingly, rather than focusing on continually improving their company's approach to security and risk management.

Cause of healthcare data breaches

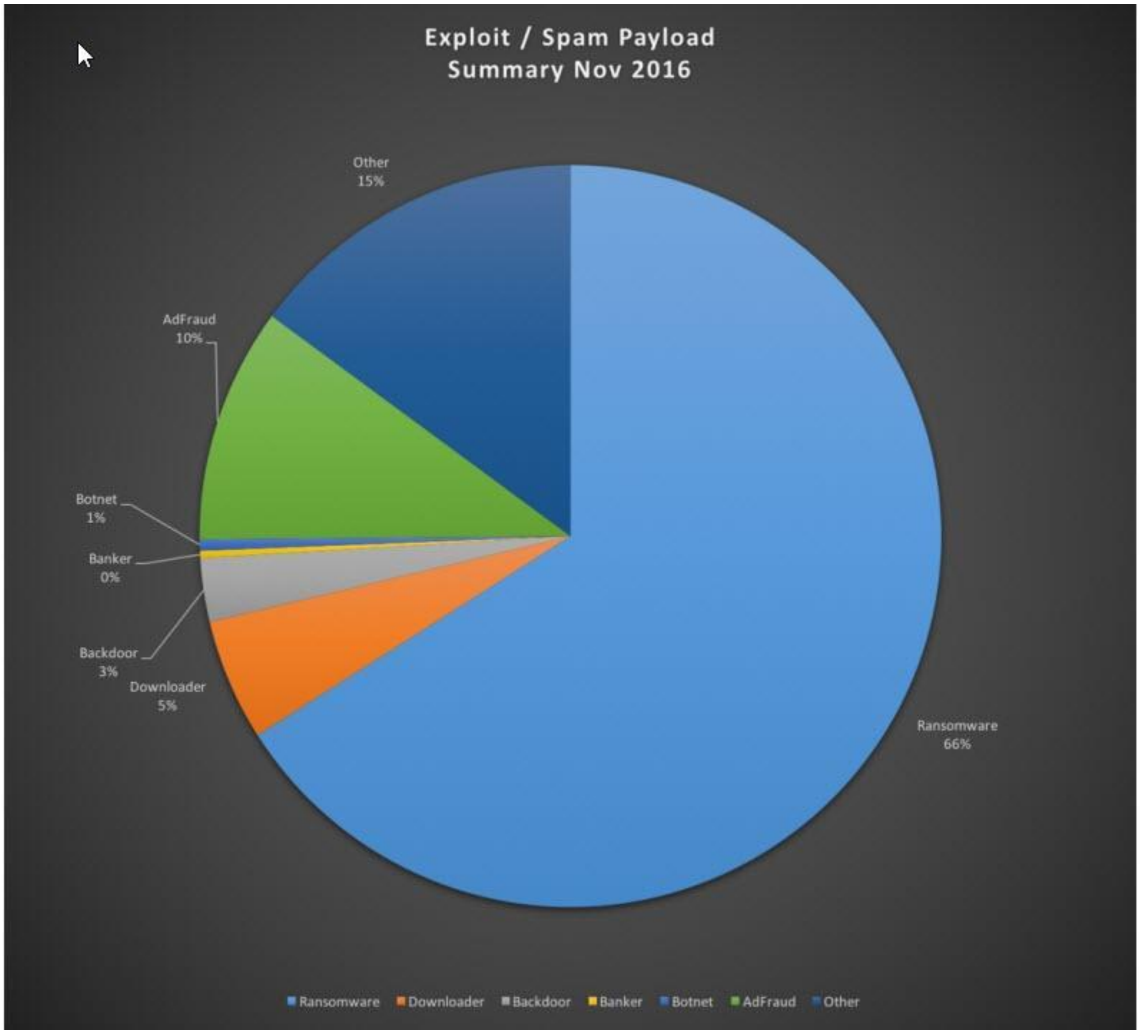
Information Systems have become core assets to almost all modern businesses; organizations are almost completely dependent on information systems to interact with the customers, deliver service, process transaction and many other business processes. Not surprisingly, this same dependency also puts organizations at greater and greater risk of a data breach. Preventing data breaches has become a nearly impossible endeavor, and healthcare organizations are by no means immune to these problems. Health records are highly sought after by criminals, and at the same time, healthcare organizations exist first and foremost to provide quality care and save lives. This often leave security as an immature process until a breach finally occurs and the affected organization resolves to better protect itself.

One of the more prominent causes of data breaches in healthcare is malware. Malware is malicious code which hackers and cybercriminals deploy in a victim's environment. In order to introduce this code, hackers must first force intended victims to launch the infected file or payload on their system. Malware then exploits software vulnerabilities to compromise computers and help attackers steal users' private data. The term malware refers to viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware or adware. These types of programs can often self-replicate or copy itself and spread automatically through an infected file; this is the most basic trait of malware. The first malware was a program called "Creeper," written by Bob Thomas in 1971 (Snyder, 2012) for fun. Creeper spread to machines connected to the ARPANET. Its purpose was rather innocent, once it found a host machine, it would use an attached teletype machine print the message "I'm the Creeper. Catch me if you can!" Although the program was harmless, it infected quite a few machines within the DoD owned ARPANET, and a year later in 1972, another programmer named Ray Tomlinson wrote a program called

Reaper to move across ARPANET and delete Creeper. Reaper, in turn, became the world first nematode or virus killer. (Snyder, 2012)

Since the 1970's Malware has become more and more complex and destructive, a multibillion-dollar industry has risen with the purpose malware detection and defense. Nation states have even weaponized viruses to attack other nation states. Many credit the United States and Israel with developing the Stuxnet virus, which attached and destroyed Iranian centrifuges engaged in uranium enrichment, causing them to vibrate until they fell apart.

To successfully introduce the payload the user must be fooled, and anti-virus programs must be evaded. Typically, antivirus solutions detect malware via signature detection, scanning functionalities, or by heuristic analysis. Malware successfully evades antivirus using several common techniques to include: adding antivirus exceptions, disabling an antivirus, using the sleep method or by using code injection. Another common evasion method is code packing and encrypting. In this method, malware authors binary tools which cause code obfuscation and by using executable packers, modern malware can completely bypass personal firewalls and antivirus scanners



https://blogs-images.forbes.com/kevinmurnane/files/2017/01/ransomware_Malwarebytes.jpg

Figure 4

Ransomware

Ransomware is another common variety of malware, but the method in which attackers use it is completely different than traditional malware. Ransomware works by preventing organizations from accessing certain parts of its system because the malware has encrypted the information contained within. Typically, organizations or it users would be locked out from critical systems, such as electronic health record (EHR). The attackers demand a sum of money to decrypt the data; usually, they require the fee in a cryptocurrency such as bitcoin. The ransom requested is often relatively small, just a few thousand dollars so in many instances the victims opt to quietly pay the fee rather than attempting to restore the encrypted data from backups. The risk of the attack becoming a breach is usually low because the attacker lacks a mechanism to extract the data from the victim's network. So, the decision to pay, even without the guarantee that the data will be unencrypted, is often made with convenience in mind.

Experts advise against paying attacker's ransom because it creates an even greater financial incentive to conduct more attacks. Never the less, ransomware attacks are becoming more numerous and destructive. WannaCry, a May 2017 malware attack infected nearly 300,000 systems worldwide. (Wong, 2017) WannaCry is a slightly more capable type malware, a cryptoworm, that has adopted the self-propagating properties of worm virus's; a cryptoworm will traverse corporate networks to find the most vulnerable targets. A 2016 virus, called Samsam, was the vanguard among this new, more potent variety of malware. (Wong, 2017) WannaCry was a more advanced variety of cryptoworm that used an attack vector called EternalBlue, which exploits a vulnerability in Microsoft's Server Message Block (SMB) protocol. (Wong, 2017) The vulnerability exists because the SMB version 1 servers in various versions of Microsoft Windows mishandles specific packets from remote attackers. WannaCry specifically exploited the unsupported Windows XP and Windows Server 2003 as well as users of the supported, but unpatched, version of Windows. When executed, WannaCry encrypts the computer's data, attempts to exploit the SMB vulnerability to spread to other computers, and finally broadcasts a message informing the user that files have been encrypted. The message demands payment in Bitcoin of around $300 within three days or $600 within seven days.

Ultimately over 200,000 computers in 150 countries were affected by WannaCry. The attack had the most substantial and potentially life-threatening effect on the United Kingdom’s National Health Service (NHS) resulting in many workers becoming locked out of their workstations and even forcing some hospitals to divert patients. In total several thousand NHS computers, running Window XP, across 42 NHS location were affected. (Wong, 2017) Ultimately the impact on the NHS as well as the Worldwide effect was relatively minimal. But the attack has made it quite clear that similar attacks, with such scale, can have potentially devastating results, especially for healthcare.

Phishing

Perhaps the most common, low cost and simple pathway for cybercriminal and fraudsters to access or steal electronic protected health information (ePHI) is by Phishing. Phishing is a variety of social engineering in which a fraudster tries to gather sensitive information, especially login credentials by masquerading as a legitimate entity or person in the email or other electronic communication. Spear Phishing is perhaps the most effective variety of the scam. In spear phishing scams, fraudsters tailor their attack to the victim by specifically using the target’s name, title, company name, phone number, etc. to trick the receiver of the message into thinking there is a connection to the sender. Often the attackers will mine this information from Linkedin, Facebook, Bio's on the official websites or other open sources, then fill contextual details that attempt to solidify the ruse. The goal in most phishing attacks is to get the victim to click on a link or open an attachment at which time a malicious payload is released or the victim inputs username and account info into a field when prompted.

John Podesta, Chairman of the Democratic National Committee (DNC), famously fell for a phishing attack before the 2016 Presidential Election. The incident led to the theft of thousands of private emails sent to and received from prominent people within the party. The attack once again was unsophisticated; Podesta received an email appearing to be from Google stating that hackers had tried to penetrate his Gmail account and recommending he changed his password immediately. Podesta wisely forwarded the email to an IT staffer inquiring if the message was legitimate. The staffer replied saying the message was legitimate; however, he meant to say "illegitimate" but left off the “i” and “l,”. The IT staffer did include a link to the official Gmail password change page and added another link at which Podesta could set up two-factor authentication, which he currently did not have in place. Unfortunately for Podesta, he inadvertently clicked on the wrong link contained in the original phishing email and unwittingly gave the attackers his username and password. As a result, hackers, believed to be Russians, stole thousands of emails which eventually made their way to WikiLeaks who subsequently released many of the emails. (Vaas, 2016)

Perhaps the most common variety of phishing is called deceptive phishing. This type of attack occurs when fraudsters create an email appearing to be a legitimate company or organization. Often, they are crafted using an organization that recipients are likely to have an account with such as a bank, Google, AT&T, etc. These emails are crafted in ways that solicit a sense of urgency from the recipient; they might say that fraudulent activity has been detected on an account or asks the recipient to click on a link redeem a limited time special offer. The goal once again is to gain login credentials or deploy a malicious payload by duping recipients into clicking on a link or downloading an attachment. While many of these emails are identified a spam and a relatively small number of the remainder fool the recipient, this scam remains popular due to the minimal effort needed to reached thousands of potential victims.

Other prominent phishing attacks include SMSishing, a variation using SMS (text) messaging. Vishing, or voice phishing, uses a voice call and often a spoofed caller ID, to gather credentials via phone. Pharming, a method in which attackers' tamper with a company's hosts files or with their domain name system files, so users are directed to fake websites even if they manually input a domain name. Once on the hoax site, the user attempts to log in, inadvertently surrendering username and login. Whaling, a phishing attack that specifically target's senior leadership who usually have privileged access. These executives often also employ poor security practices, due to the fact they do not always partake in security training and education, leaving them especially vulnerable.

The Future Vulnerability of Medical Devices

Perhaps no new technology in healthcare has industry leaders more concerned than medical devices. Medical devices play a critical role in modern health for the prevention, diagnosis, treatment, and rehabilitation of disease and illness. A medical device is “an instrument, apparatus, implement, machine, implant, in vitro or other similar articles, including a component part, or accessory manufacturers.” (FDA Basics, 2015), A device must also be recognized in the official National Formulary or the United States Pharmacopoeia. It must be used in the diagnosis, cure, mitigation, treatment, or prevention of disease, in man or other animals.

Today there are over 25 million implantable medical devices (IMD) in use in the United States. They include devices such as cardiac defibrillators, pacemakers, coronary stents, artificial hips, artificial knees, and neurostimulators. Implanting devices in human beings considerably increase the need for reliability and device security, because of the life providing nature of many of these devices. Medical devices started to see widespread use by the 1980's. Concerns regarding safety and privacy emerged in the 1980’s as well. In 1987 radiation therapy machine known as a Therac-25, caused radiation poising in a number of patients, the caused was determined to be the result of programming errors. (Burns 2016, p. 1) By the turn of the century, a specific category of medical devices, which are implanted and networkable, began to emerge. These devices in particular really began to make people in the healthcare industry concerned about cybersecurity.   By the year 2000, over 114,000 cardiac defibrillators had been recalled by the FDA. Several deaths have been attributed to faulty defibrillators including the 2005 death of a Minnesota college student. (Robbins 2017)

By the early 2000s, over half of medical devices were software driven. Many of the implantable devices became wirelessly networkable so that patches, updates, and setting changes could be made without surgically removing the device. By 2008, a number software security flaws began to come to light with these devices, most noticeably with Implantable Cardiac Defibrillators (ICDs). These vulnerabilities allow for the possibility of both electronic eavesdropping and even for third-party control of the ICD's operation. Initially many of these devices exclusively used Radio frequency (RF) signals to communicate remotely with the device. This method typically requires a specialized wand that must be in very close proximity to communicate with the device. However, manufacturers began to replace RF communications with Wi-Fi communication, this had numerous benefits, for instance, it allowed devices to be continuously monitored to obtain device status or patient status, and it allowed changes in setting or software updates to be made remotely. Typically, an ICD user has a wireless transmitter in their home instead of the wand, while this transmitter still has to be relatively close the ICD, but the WiFi ICD capable of receiving signals from much greater distances in the old RF technology.

Fear over third-party control was depicted in a 2012 episode of the television show Homeland, in the episode, the Vice President of the United States is killed after a group of hackers remotely accessed his ICD and caused it to send lethal levels of electric shock. The episode most likely drew its inspiration from former Vice President Dick Cheney; the Secret Service had the Wi-Fi functionality of his pacemaker turned off to prevent this type of attack. Currently, networkable IMD security is a major concern among security professional in the healthcare industry.

While the episode of Homeland may have been a bit of Hollywood fiction, Barnaby Jack proved that there were real-life concerns for IMD security (Burns 2016, p. 5). In 2012, during Ruxcon Breakpoint Security Conference in Australia, Jack exhibited a video presentation during which he demonstrated he could deliver an 830-volt shock from a pacemaker using its wireless transmitter. Jack found that certain devices could even be accessed simply by using the device's a serial number and model number. While potentially lethal vulnerabilities inevitably generate the most fear, the fact that these devices can be so easily hacked makes them potential targets for malicious hackers looking for personal information.

FDA and Medical Devices

While manufacturers of IMDs have long been aware of security concerns present in IMD, fixing flaws has not always been easy because regulation of IMDs falls under the responsibility of the Food and Drug Administration (FDA). A serious point of contention has long been post-market security and software updates. The FDA treated these modifications the same as it would treat medication when its formula changed, after which the medication must go through the FDA's testing and the trial process all over again. Similarly, when an IMD’s software is modified, that device must be re-tested before it is approved for the marketplace. This requirement creates an incredibly bottlenecked process to make changes to IMD’s when security flaws in its software are discovered.

A 2008 supreme court case, Riegel v. Medtronic, Inc. further compounded the issue of addressing IMD security flaws. In the case, the patient brought common law claim against the manufacturer of a faulty medical device that had been FDA approved. The device, a simple balloon catheter, rupture in the patient's artery during an angioplasty. The plaintiff sued the device manufacturer Medtronic, but the courts found in favor of the defendant. The outcome of the ruling essentially exempts device manufacturers from state-based legal claims for faulty medical devices that have been approved by the FDA. So, this even further complicated the likelihood that medical device vulnerabilities would be quickly fixed. The FDA’s process slows down the rate at which software is updated and the device manufacturers have at least perceived exemption from liability once a device is approved by the FDA. (Burns 2016)

By 2013 the FDA had begun to develop specific guidance for medical device manufacturers to consider, following preliminary feedback from a series of medical device cybersecurity workshops held the previous year. The FDA recommended that manufacturers implement a structured and systematic cybersecurity risk management program and respond quickly once vulnerabilities were discovered. The specific recommendation included the following:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies; and
- Assessment of residual risk and risk acceptance criteria. (Burns 2016)

Unfortunately, this guidance focused specifically on the pre-market environment and were not mandatory measures. Because risk and threats to medical devices are continually evolving, it is almost impossible to completely mitigate those during the device's design phase. It was not long before cyber security experts began advocating for more new methods of protecting these increasingly complex devices.

Finally, in January 2016 the FDA released draft guidance covering post-market cybersecurity for medical devices. The new guidance emphasizes that the device manufacturer's role does not end once the device has been approved by the FDA and it establishes that the FDA expects device manufacturers to continue to provide security support to devices after they have been released. The guidance also clearly outlined that although software redesigns will require FDA approval, security patches will not and the FDA encouraged manufacturers to continue to issue security patches when vulnerabilities are discovered. It also emphasizes the expectation that manufacturers will gather and share information about cybersecurity threats with one another. Additionally, the guidance recommends that device manufacturers should employ a systematic cybersecurity risk management program for their supported devices and respond timely to identify threats and vulnerabilities. The NIST Cybersecurity Framework was specifically recommended for use; the framework prescribes that practitioners use the following cycle of steps for security: identity, project, detect, respond, then recover. Finally, the guidance recommends the following critical components that such a program should include:

- Applying the 2014 National Institute of Standards and Technology Voluntary Framework for Improving Critical Infrastructure Cybersecurity;
- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation. (McGee 2016)

While the FDA’s guidance is voluntary, failure to comply could result in a violation of the quality systems requirements of the FDA's Food Drug and Cosmetics Act. More importantly, the guidance highlights the absolute importance of the device security and the stakes at play. The healthcare industry has long understood its fiduciary responsibility to the health of patients, so hopefully, this mindset will better position the industry to tackle cyber security. Ultimately medical device security is a shared responsibility between device manufacturers, healthcare organizations and the FDA. Device manufacturers have a responsibility to protect intellectual property, secure devices, and protect their reputational integrity. Healthcare organizations have a responsibility to provide quality care safely and affordably. The FDA has the responsibility to oversee industry protect consumers.

The Way Ahead: People, Process, Technology

What can organizations do to reduce the likelihood of suffering a breach? Many industry leaders have observed an over-reliance on technology; technology in and of itself has not reduced the instances of breaches. But, Organizations too often believe that breach prevention is solely an IT problem and subsequently deploy technological solutions to address vulnerabilities. However, some security leaders, in the industry, have begun to emphasize more holistic or employee centric approaches to security. One popular method is the People-Process-Technology Triad, the concept emphasizes that good security is predicated on a foundational overlap of those three elements. (Brink 2016)

Technology plays a central role in information security. Organizations employ many solutions for security such as security information and event management (SIEM) solutions, intrusion detection system (IDS / IPS), log analysis tools, vulnerability scanning, Data Loss Prevention (DLP), Patching, Anti-Virus, Email Filtering and encryption. But these technology implementations cost money and have a low return on investment (ROI). Thus, many companies are slow to implement these solutions, others don't have the budget at all, and many public sectors organization have to plan a budget way advance and are consequently often years behind in introducing solutions.

The people portion of the triad focuses on employees and users who not only have an important role in preventing data breaches but also are often a contributing factor when breaches occur. An Employee opens an email which launches malicious payload, a lab top is stolen, a thumb drive is lost, an email with PII is sent to the wrong addresses, etc. The vulnerability of an untrained, unsophisticated workforce must first be addressed so that technological solutions can be fully effective. Training of the workforce is often hastily given during new hire orientation or not provided at all. Annual refreshers or training reminders are also often glossed over leading to a workforce that is not aware of new and emerging vulnerabilities. Many organizations also struggle to effectively manage use and accountability information system access amongst employees, contractors, and temp employees. Privilege access management is also a people-centric activity that many organizations struggle with, accidental or deliberate misuse of these elevated accounts is so often a contributing factor in breach events.

Finally, we have processes which are the procedures, operations, and steps an organization undertakes in support of its security program. Process include activities such as conducting a risk assessment, background check on employees, IT governance, change management, incident response and contingency operations. These processes help drive successful security programs.

These three elements of people, process, and technology must be in alignment with security to be most effective. This was notably the case in the aftermath of the 2014 Target data breach. Target employed an expensive and elaborate set of technological security solutions, spent hundreds of millions on security, had been recently certified as PCI compliant and was even running its own security operations center. One particular solution, Dynamic Treat Intelligence (DTI) by FireEye had been in place for about a year and was considered a top of the line security tool. DTI caught the first penetration on November 30, 2014, within Target's payment system. More than five alerts went off that were rated at the top of DTI's criticality scale, the alerts were seen by Target security teams in both India and Minnesota but were ignored. (Radiche 2014) Why were the alerts ignored? Because, in addition to 5 alerts received on November, 30th, Target received hundreds of other alerts on DTI as well as numerous alerts from other systems. An alert by itself is not simply enough. A security team needs to be properly employed in order to understand the risks represented by specific threats and subsequently make the recommendation and prioritize. Target over-relied on technology. In this case, Target made the appropriate investment in "technology" but arguably did not put the appropriate emphasis on people and processes.

Target could have better prepared the "people" who were working in the organization's security office. It also could have improved it's "processes" specifically the original cause of the breach, an HVAC vendor that was given external network access, leading to the initial penetration by the attackers.

Boston Children’s Hospital, an example of a good P/P/T

A 2014 security incident involving Boston's Children's Hospital is a fantastic antidote for how emphasizing good processes can greatly aid an organization in times of emergency. The incident stemmed from the controversial custody battle of Justina Pelletier who was diagnosed with mitochondrial disease. She was treated by Doctors at Boston Children's who disputed the diagnosis and accused her parents of medical child abuse. Somatoform Disorder was instead diagnosed with the hypothesis that her symptoms were psychological and not real at all. The state intervened and stripped the parents of custody; she was subsequently held at the Hospital’s Psychiatric ward, where she remained over a year.

The incident drew the attention of the hacker group known as Anonymous who believed Justina was unjustly detained. Before the attack started, Anonymous posted a warning on Twitter with the group's demands, they wanted the hospital to terminate Doctor Alice Newton, the physician they held responsible, and to release Justina to her family. When the hospital did not meet the demands, Anonymous launched #OpJustina. They commenced the attack by publicly releasing the contact info and PII of Judge Joseph Johnson, who made the court ruling, and Doctor Newton, a tactic called “Doxxing,” as well as technical info about the hospital’s website.

Anonymous then used the information it possessed about the hospital's website to launch a Distributed Denial of Service (DDoS) attack on the hospital's public-facing sites. DDoS attacks are designed to overwhelm the sites and make them unusable. Anonymous then escalated the attack with the use of direct penetration attacks and spear phishing emails in the attempt to get users to click on links or open attachments allowing hackers access to portions of the network behind firewalls.

Boston Children's Hospital had its back against the wall at this point; many companies would have partially given in to the attacker's demands to avoid a potential catastrophe, but the hospital didn't give in, instead choosing to fight back. Chief Information Officer, Dr. Daniel Nigrin, along with Hospital's Insistent Response Team, began making preparation as soon as threats were made against the hospital, the preparations included the option of taking the hospital entirely offline or going completely dark if necessary. The hospital initially handled the DDoS attacks on its own, then used a third-party security service whose services were pre-arranged. The Hospital then took down all public facing websites and shut down email, instead of using a recently deployed secure text messaging application. (Eastwood 2014)

The hospital then held firm and prepared for Anonymous' next move, it never came. Within Anonymous, which is a coalition of like-minded people rather than a hierarchal organization, there was apparently some disagreements amongst its member on whether or not the Hospital should be attacked. Approximately ten days after the attack commenced, a message went out from the groups' twitter account "To all the "Anons" attacking the CHILDREN'S HOSPITAL in the name of Anonymous via Op #JustinaPelletier - IT IS A HOSPITAL: STOP IT." (Kushner 2017)The attacks ceased suddenly after the message, the attackers never gained access to any PII, and the hospital's Electronic Health Records System (EHR) was never impacted and remained online.

Boston's Children's Hospital successfully dealt with this deliberate attack by skilled hackers because it had good processes. The hospital's contingency plans were well thought out and well-rehearsed. Its leadership trained and prepared for scenarios like this, or perhaps even more complicated than this. Certainly, the organization benefited from a bit of luck, as the hackers self-policed themselves rather than escalating even further. However, the hospital's emphasis on people, process, and technology, rather than on technology only, played a critical role in its favorable response to the attack.

Safesforce, a culture of security

Savvy organizations are beginning to emphasize the human factors of security; however, healthcare is rarely on the cutting edge of organizational innovation. In 2012 Salesforce.com, a company that specializes in customer relationship management (CRM) software, began to adopt a new, innovative approach to creating a more effective information security program. Salesforce sought to improve upon the practice of simply training workforce members on security practices and instead it sought to revolutionize culture so that all employees would embrace their role security. In this pursuit, Salesforce created a culture of security, a distinct difference from a culture of compliance, which is focused only on meeting regulatory rules. Salesforce created a group called the security behavior team, whose job was to focus on people and processes to improve security. Salesforce's approach included emphasizing security-minded behavior, innovating education with the use a Learning Management System and most importantly by the gamification of security where employees were rewarded for engaging in security challenges or reporting technical vulnerabilities. What Salesforce did, in effect, was solve the human factor. Most organizations do the technical aspects of security well or pay someone else to do so. The human factor, on the other hand, is difficult to understand or master, even for companies with deep pockets. (Sedova, 2016)

Mastering the human factor is the aspect of information security that the health care struggles with most. Information security leaders in healthcare are fixated on compliance, with HIPAA. The goal of the organization's security program, in these cases, becomes meeting administrative, technical and physical security regulations rather than preventing breaches. The primary goal of a mature information security program should be to understand the threats and vulnerabilities, determining which could cause the most harm, and assessing which are most likely to occur. A compliance-based approach typically leads to the adoption of various technical controls and the development of possesses and procedure simply for the sake of including them in policy. Training for new employees is often the limit of the focus on people. But people and process enable that technical solution to function effectively, and it takes savvy leadership to bring the three factors people, process together. Salesforce' approach involved picking vital behavior, connecting it to purpose, testing and giving feedback, rewarding success, recognizing and socializing this behavior.

Compliant cloud computing can aid Healthcare

Cloud computing is another technology that has seen widespread adoption in recent years, although healthcare has been more apprehensive about adopting cloud than other industries, most large healthcare organizations are using the cloud in some capacity. The National Institute for Standards and Technology (NIST), describes cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." In simple terms cloud computing refers to accessing data, or programs through the internet rather than on a computer's hard drive or a local file server.

Cloud Computing can be divided into three activities, storage, computing, and networking. These activities are often further classified by location, private or on premises, public, and hybrid. Another common categorization is Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). IaaS is just that, space on servers in a data center carved out for use. Notable examples include Microsoft Azure, Rackspace and Amazon Web Services. This appeals to organizations who simply want to remove the need to have a large on-site data center; the servers can be configured to do nearly anything the client desires. PaaS provides an environment for companies to create, host and deploy applications easily without having to maintain complex infrastructure, examples include Google app engine and Heroku. SaaS is simply software that is hosted offsite and designed by a third party; examples include SalesForce and Google suite.

One of the major factors in the apprehension to adopt cloud services, among many healthcare organizations, is the mistaken belief that cloud is less secure than locally hosted solutions. In reality, this is not typically the case, in fact, on-premise solutions tend to encounter more breaches because the organization is typically responsible for security management for that system. Whereas reputable cloud vendors tend to have very good at security procedures. This is because their livelihood, as a business depends, on having a good security reputation and because they tend to employ more dedicated security staff members than the typical healthcare Company. Also from a physical security perspective, a cloud vendor's data Center is likely to be significantly more secure than data centers located in a hospital which may only have an exterior door facing a public area as the only security control.

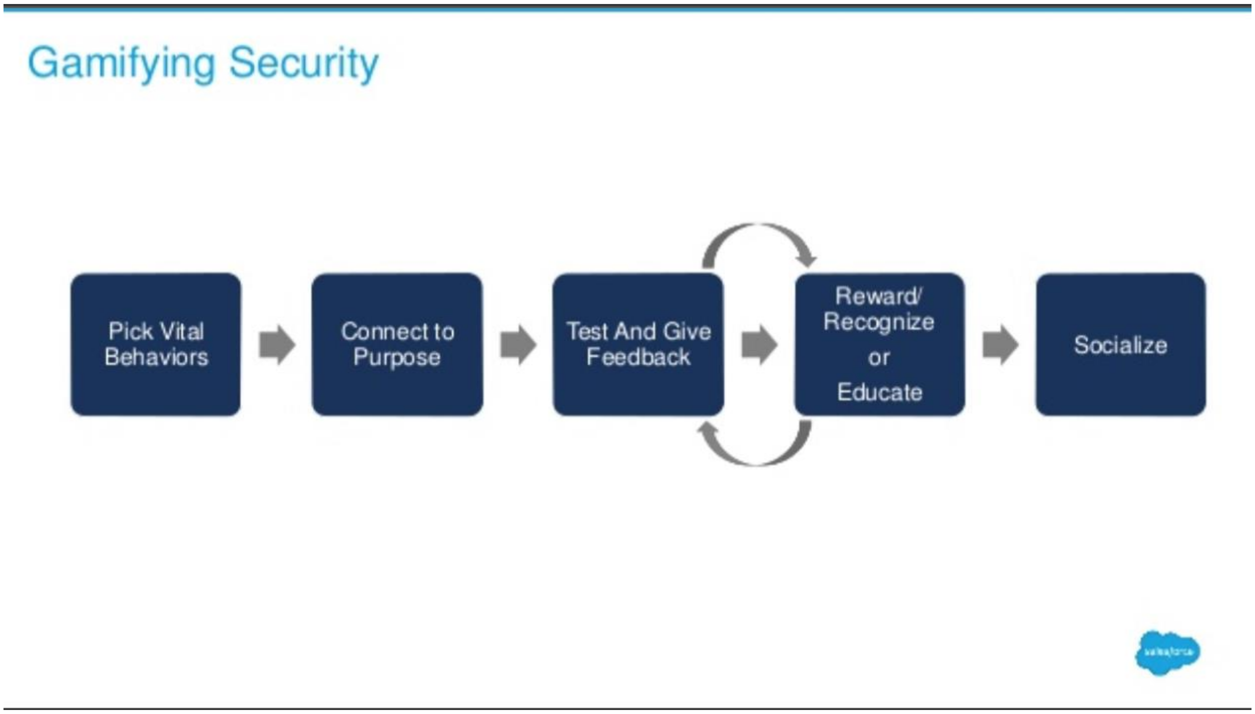
Despite a belief by many that storing ePHI in a cloud environment is less secure, the opposite may be true. According to a 2013 Cloud Security Report by Alert Logic, the on-premises users experienced an average of 61.4 attacks a year, while cloud user experienced just 27.8 per year. Both cloud and on-premises set up can be equally be targeted by hackers, but the variation in incidents can be credited to several factors. Security controls for cloud storage are more consistent than with on-premises solutions. Physical security is stronger as the actual servers are housed in a very secure remote data center. In many older hospitals, these centers are often located in rooms not originally designed as a data center. These centers are overly cramped, have poor environmental controls, use water based fire suppression and may even have large water mains and other pipes passing overhead. Often non-IT personnel such as maintenance folks have full access. Even worse, many small clinics and providers are using shared data centers in the office space they lease. Technical security can also be a problem, often times healthcare organization have an understaffed IT workforce and IT security almost always understaffed or assigned as a collateral duty. Lack of funding may also mean Healthcare organization are relying on older, outdated security solutions. Cloud vendors, for the most part, have better security than the average the healthcare organization and often employ a wide range of security monitoring tools that are too expensive or under-utilized by their staffs.

There is also a perception that Data stored in the cloud is more vulnerable to hackers. This attitude has gained widespread acceptance in light of the number of high-profile cloud leaks, such as the 2014 iCloud leak. In the iCloud leak, photos of dozens of celebrities were leaked after their passwords were hacked. Lack of visibility, because the data is not stored on site, also contributes to a perception of lack of control. But in reality, most healthcare data stored on premise is still networked and access can be gained without being physically at the location. But many cloud providers employee a defense in depth approach to data security which many healthcare organizations are unable to match themselves because IT is not a core competency of many healthcare providers. Quite simply, most healthcare organizations are unable to match the resources that are employed by cloud providers. Additionally, many cloud providers undergo a number of rigorous security certifications, such as HITRUST, that few healthcare providers ever obtain.

Cloud also has some other advantages that cannot be matched by on-premises solutions when it comes to the confidentiality, integrity, availability (CIA) triad. Cloud contributes significantly to health information exchange (HIE), HIE is a healthcare concept that allows providers and patients to both access and share electronic medical records across an organization, within a region, community or hospital systems. Cloud environments, by design, allow an auditable chain of custody for your data at a high level. Cloud data may traverse many different data centers region or can be hosted multiple places simultaneously so strong audit and log management if necessary.

Another deeply rooted aversion is due to the myth of trust. Many organization simply believe that they cannot trust an outside organization. But in reality, an organization's own workforce sometime represents one of its biggest vulnerabilities. While storing data in the cloud doesn’t eliminate those vulnerabilities, the security mechanism of any reputable cloud vendor is better that of many healthcare organizations.

Finally, the cloud can simplify HIPAA compliance. The HIPAA security rule requires healthcare organization to comply with a host of technical regulations, some which can be rather costly and manpower intensive. The average healthcare organization has an understaffed IT security workforce and the HIPAA security rule requires the review of audit logs generated when ePHI is access or modified. A typical healthcare organization may have thousands, even tens of thousands of audit logs generated on a daily basis. Conducting reviews of even a portion of those log entries is difficult. The same goes assigning and auditing user accounts and user access. Organizations can purchase expensive auditing and log management solutions, expensive identity and access management solutions or expensive encryption solutions. However, a reputable cloud vendor would like to employ these solutions and is more likely to have the appropriate staff to utilize them.



Gamifying Security

Pick Vital Behaviors

Connect to Purpose

Test And Give Feedback

Reward/ Recognize or Educate

Socialize

Figure 5
(Sedova 2016)

Conclusion

The mind field that healthcare information security professionals must navigate is a challenging one, but the industry can do many things to help balance the people-process-technology triad and reduce breaches. The first step is hiring the right people for the job. Far too often CISOs in healthcare come from the network security ranks. While those employees may be perfectly adequate for the job, the qualification of a CISO does not necessarily require many of the hard skills possessed by a network security specialist. Far more desirable is a quality leader who can effectively lead and manage in a high-risk environment. It is far easier for a manager to learn technical skill sets or leave those skills sets to specialists than it is to impart quality leadership skills on a network security specialist. The same is true for the security staff; an ideal team is made up of individuals with diverse skill sets and talents, who also come from diverse backgrounds which include industry's outside of healthcare. The are many talented folks outside of the healthcare industry that can be tapped to help organizations build strong security teams.

With the right team in place, another critical action is the smart, focused investment in information security tools. Far too often organizations purchase expensive security tools which they are barely capable of employing to the full extent. This is either because the tools are too complex or because the organization doesn't have the time or staff to adequately utilize the tool. Tools such as penetration testers, email filters, vulnerability scanners, log analysis tool, etc., are purchased before an organization decides it should develop a strategy to effectively employ those tools. Many organizations are using 8-10 different security solutions, all pumping out logs and alerts constantly. Consequently, alerts or automated log reports pile up without getting vetted or reviewed. Security solutions that aren't monitored or adequately managed become security problems in these cases. Instead, organizations should develop a smart strategy for employment of technical solutions, then determine the appropriate resources to devote to ensuring its solutions are deployed efficiently.

When breaches make headlines, the narratives tend to be about criminal hackers or some catastrophic failure in technology. This narrative is easy for the victimized organization to understand and is also beneficial when explaining a breach to customer and shareholder. However, organizations need to fully embrace the idea that their biggest cybersecurity threat is not a shadowy group of transnational hacker, but instead, the organization's own employees. A renewed focus on employees is perhaps the most effective step organizations can take to improve security. Organizations can take three simple workforce centric steps to improve security: 1) Get buy-in from executives (before a breach). Quality training isn't free, implementing a mature security and awareness training program can seem cost prohibitive or may divert funding from competing needs. Buy in is crucial in ensuring that information security is financially supported to the proper extent. Also developing a corporate ethos in support of security requires support from the top, otherwise cultural change is not possible. 2) Foster a Culture of security, most organization employ a culture of compliance which focuses on meeting regulatory requirement. Regulatory requirements are rarely adequate for preventing a breach and are minimum standards at best. A culture of security focuses on being aware of emerging threats, understanding individual employees' role in security and employing best practices to prevent breaches. 3) Finally, incentivize security, reward employees for identifying security vulnerabilities, doing well on security quiz or training, and performing the best on security assessments and audits. Security is important, so motivating employees through means other than sanctions for violation can be an incredibly effective technique.

Once leaders in the healthcare fully embrace the cultural changes necessary to improve security and put a renewed focus on people, process, and technology integration, the industry may finally see instances of security breach drop. Until then, the industry will continue to make headlines with significant and costly breaches.

Bibliography

1. L. V. (2017, May 30). Security of medical devices ‘is a life or death issue’, warns researcher. Retrieved September 12, 2017, from https://nakedsecurity.sophos.com/2017/05/30/security-of-medical-devices-is-a-life-or-death-issue-warns-researcher/

2. Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management, 6*(4), 279. doi:10.1504/ijiem.2010.035624 http://www.inderscienceonline.com/doi/abs/10.1504/IJIEM.2010.035624

3. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627 McGee , M. K. (2017, January 10). A New In-Depth Analysis of Anthem Breach. Retrieved October 12, 2017, from https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

4. Meiling, B. (2015). Anthem Discloses Data Breach. *San Diego Business Journal*, *36*(6), 3. http://te7fv6dm8k.search.serialssolutions.com/?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummon.serialssolutions.com&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rft.genre=article&rft.atitle=Anthem+discloses+data+breach&rft.jtitle=San+Diego+Business+Journal&rft.au=Meiling%2C+Brittany&rft.date=2015-02-09&rft.pub=CBJ%2C+L.P&rft.issn=8750-6890&rft.volume=36&rft.issue=6&rft.spage=3&rft.externalDBID=IOF&rft.externalDocID=403050224&paramdict=en-US

5. A True Medical Emergency: Diagnosing the Anthem Security Breach. (2015, December 02). Retrieved September 12, 2017, from https://diamondit.pro/network-security/a-true-medical-emergency-diagnosing-the-anthem-security-breach/

6. Brook, C., & About Chris Brook "Distrust and caution are the parents of security" - Benjamin Franklin View all posts by Chris Brook →. (2017, June 26). Anthem Agrees to Settle 2015 Data Breach for $115 Million. Retrieved September 12, 2017, from https://threatpost.com/anthem-agrees-to-settle-2015-data-breach-for-115-million/126527/

7. Knippa, P. (n.d.). What Healthcare Can Learn From CHS Data Breach. Retrieved September 12, 2017, from https://www.informationweek.com/healthcare/security-and-privacy/what-healthcare-can-learn-from-chs-data-breach/a/d-id/1317696

8. Young, B. (2016, December 21). Data breach exposes info for 400,000 Community Health Plan members. Retrieved September 12, 2017, from http://www.seattletimes.com/seattle-news/health/data-breach-exposes-info-for-400000-community-health-plan-members

9. Melnik, T. (2012, June). Class Actions, Federal Actions, and State Actions: The Data Breach Saga Continues. Retrieved September 12, 2017, from http://te7fv6dm8k.search.serialssolutions.com/?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummon.serialssolutions.com&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rft.genre=article&rft.atitle=The%2Bdata%2Bbreach%2Blawsuits%2Bbegin%3A%2Bclass%2Baction%2Blawsuit%2Bfiled%2Bagainst%2BSutter%2BHealth%2Band%2Bthe%2BUCLA%2BHealth%2BSystem%3A%2Borganizations%2Bmust%2Bdo%2Beverything%2Bthey%2Bcan%2Bto%2Bensure%2Bcompliance&rft.jtitle=Journal%2Bof%2BHealth%2BCare%2BCompliance&rft.au=Melnik%2C%2BTatiana&rft.date=2012-03-01&rft.pub=Aspen%2BPublishers%2C%2BInc&rft.issn=1520-8303&rft.volume=14&rft.issue=2&rft.spage=45&rft.externalDBID=IAO&rft.externalDocID=350166776¶mdict=en-US

10. Sutter Health sued for $1 billion following data breach -. (2013, September 18). Retrieved September 12, 2017, from http://blog.trendmicro.com/sutter-health-sued-for-1-billion-following-data-breach/

11. Causes of breaches. Ayyagari. (2012). An Exploratory Analysis of Data Breaches From 2005-2011: Trends and Insights. *Journal of Information Privacy & Security, 8*(2), 33-56. Retrieved September 12, 2017.https://search-proquest-com.ezproxy.lib.utexas.edu/docview/1086344058?pq-origsite=summon

12. Belliveau, H. J. (2016, April 27). Human Error Leading Cause of Healthcare Data Breaches in 2015. Retrieved September 1, 2017, from https://healthitsecurity.com/news/human-error-leading-cause-of-healthcare-data-breaches-in-2015

13. Survey Cites Human Error as Biggest Cause of Data Breaches. (2015). *Information Management Journal;, 49*(12), 12-14. doi:10.1075/ps.5.3.02chi.audio.2f http://te7fv6dm8k.search.serialssolutions.com/?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummon.serialssolutions.com&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rft.genre=article&rft.atitle=Survey+Cites+Human+Error+as+Biggest+Cause+of+Data+Breaches&rft.jtitle=Information+Management&rft.au=Anonymous&rft.date=2015-07-01&rft.pub=ARMA+International&rft.eissn=2155-3505&rft.volume=49&rft.issue=4&rft.spage=12&rft.externalDocID=3743459461&paramdict=en-US

14. STRAUSS, L. (2015). Data Breach Study: Criminal Attacks Now Leading Cause. *Journal of Health Care Compliance, 17*(5), 61-65. Retrieved from

http://te7fv6dm8k.search.serialssolutions.com/?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummon.serialssolutions.com&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rft.genre=article&rft.atitle=Data Breach Study%3A Criminal Attacks Now Leading Cause&rft.jtitle=Journal of Health Care Compliance&rft.au=Lori J Strauss&rft.date=2015-09-01&rft.pub=Aspen Publishers%2C Inc&rft.issn=1520-8303&rft.volume=17&rft.issue=5&rft.spage=61&rft.externalDocID=3818615921¶mdict=en-US

16. Ring, T. (n.d.). A breach too far? Retrieved September 12, 2017, from http://www.sciencedirect.com/science/article/pii/S1361372313700526?via%3Dihub

17. Snyder, D. (2012, July 24). The very first viruses: Creeper, Wabbit and Brain. Retrieved July 31, 2017, from http://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain/

18. Wright, J. (2016). Ransomware: taking businesses hostage. *Network Security, 2016*(10). Retrieved from http://www.sciencedirect.com.ezproxy.lib.utexas.edu/journal/network-security/vol/2016/issue/10

19. Wong, J. C., & Solon, O. (2017, May 12). Massive ransomware cyber-attack hits nearly 100 countries around the world. Retrieved October 30, 2017, from https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

20. Spring, T. (2016, April 12). Meet The Cryptoworm, The Future of Ransomware. Retrieved October 30, 2017, from https://threatpost.com/meet-the-cryptoworm-the-future-of-ransomware/117330/

21. Bisson, D. (2016, June 03). 6 Common Phishing Attacks and How to Protect Against Them. Retrieved October 30, 2017, from https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

22. Vaas, L. (2016, December 16). DNC chief Podesta led to phishing link ‘thanks to a typo’. Retrieved August 1, 2017, from https://nakedsecurity.sophos.com/2016/12/16/dnc-chief-podesta-led-to-phishing-link-thanks-to-a-typo/

23. Snell, E. (2016, December 14). How Ransomware Affects Hospital Data Security. Retrieved September 13, 2017, from https://healthitsecurity.com/features/how-ransomware-affects-hospital-data-security

24. Mukherjee, S. (2017, May 15). Why Health Care Is Especially Vulnerable to Ransomware Attacks. Retrieved September 13, 2017, from http://fortune.com/2017/05/15/ransomware-attack-healthcare/

25. Munro, D. (2016, January 04). Data Breaches In Healthcare Totaled Over 112 Million Records In 2015. Retrieved October 23, 2017, from https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#16369667b07f

25. Sittig, D. F., & Singh, H. (2016). A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Retrieved September 13, 2017, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4941865/

26. Habtamu Habtamu, A. (2012, January). Risk-based adaptive security for smart IoT in eHealth. Retrieved September 13, 2017, from http://dl.acm.org/citation.cfm?id=2442752

27. Xiali Hei, Xiaojiang Du. (2013). Security for Wireless Implantable Medical Devices. New York, NY. Springer.

28. Bathurst, R. (n.d.). *The Medical Device Paradox Hospital Systems & Device OEMs Race Against Time to Close the Patient Safety Cyber Gap*. doi:https://www.cylance.com/content/dam/cylance/pdfs/case_studies/HealthCare_Whitepaper_2.pdf

29. Digital Health – Cybersecurity center for Devices and Radiological Health - https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

30. Medical Device Innovation, Safety and Security Consortium http://www.mdiss.org/

31. Safety Communications - Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication (2017 9, January) Center for Devices and Radiological Health- https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

32. Center for Devices and Radiological Health. (n.d.). Safety Communications - Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication. (2015 May13). From https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm

33. Becker, R. (2016, December 27). New cybersecurity guidelines for medical devices tackle evolving threats. From http://www.theverge.com/2016/12/27/14095166/fda-guidance-medical-device-cybersecurity-cyberattack-hacking-guidelines

34. Symantec™ Industry Focus: Medical Device Security (2016) https://www.symantec.com/content/dam/symantec/docs/data-sheets/symc-med-device-security-en.pdf

35. Higgins, K. J. (2016, January 20). Medical Device Security Gets Intensive Care. Retrieved March 01, 2017, from http://www.darkreading.com/iot/medical-device-security-gets-intensive-care/d/d-id/1323989

36. Medical Device Security. (2016, December 29). Retrieved March 01, 2017, from http://www.himss.org/medical-device-security

37. Jones, R. L. (2016, November 28). Medical device cybersecurity | Deloitte US | Deloitte Center for Health Solutions. https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/center-for-health-solutions-networked-medical-device-cybersecurity-and-patient-safety.html

38. McGee, M. K. (n.d.). FDA Issues More Medical Device Security Guidance. Retrieved January 18, 2016, from http://www.databreachtoday.com/fda-issues-more-medical-device-security-guidance-a-8805

39. Johnsom, M. E. (2017, February 27). Retrieved March 01, 2017, from https://vimeo.com/181070016

40. Robbins, G. (2017, January 11). Retrieved March 01, 2017, from http://www.sandiegouniontribune.com/sd-me-heartdevice-hacking-20170111-story.html\

41. Burns, A. J. (2016, October 01). A Brief Chronology of Medical Device Security. Retrieved March 31, 2017, from http://cacm.acm.org/magazines/2016/10/207766-a-brief-chronology-of-medical-device-security/fulltext

42. Center for Devices and Radiological Health. (n.d.). FDA Basics - What is a medical device? Retrieved December 28, 2015, from https://www.fda.gov/aboutfda/transparency/basics/ucm211822.htm

43. Gold, J. (2017, August 03). IoT security for healthcare is in critical condition. Retrieved September 13, 2017, from https://www.networkworld.com/article/3212991/internet-of-things/iot-security-for-healthcare-is-in-critical-condition.html

44. Griebel, L., Prokosch, H., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., . . . Sedlmayr, M. (2015, March 19). A scoping review of cloud computing in healthcare. Retrieved November 30, 2017, from https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-015-0145-7

46. Asija, R., & Nallusamy, R. (2016). Healthcare SaaS Based on a Data Model with Built-In Security and Privacy. *International Journal of Cloud Applications and Computing,6*(3), 1-14. doi:10.4018/ijcac.2016070101 https://www.igi-global.com/article/healthcare-saas-based-on-a-data-model-with-built-in-security-and-privacy/159834

47. Understanding The Cyber Kill Chain – Cloud Security Report. (n.d.). Retrieved July 27, 2017, from https://www.alertlogic.com/resources/cloud-security-report-2015/ 1

48. Brown, E. A. (2016, September 21). Final Version of NIST Cloud Computing Definition Published. Retrieved July 27, 2017, from https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

49. Secretary, H. O., & (OCR), O. F. (2013, July 26). Summary of the HIPAA Privacy Rule. Retrieved July 12, 2017, from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

51. Wang, K. (2010, September 2). Trusted Cloud Computing with Secure Resources and Data Coloring. Retrieved July 27, 2017, from http://ieeexplore.ieee.org/abstract/document/5562490/

52. Scholl, M., Stine, K., & Hash, J. (2008, October 1). *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* [Scholarly project]. In *NIST 800-66*. Retrieved June 14, 2017, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

53. Bisson, D, Oct 2, 2016Featured Articles, D. (2016, October 03). People, Processes & Technology: An Organization's Cyber Security Triad. Retrieved September 13, 2017, from https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/people-processes-and-technology-the-triad-of-your-organizations-cyber-security/

54. Brink, D. (2016, February 10). A Strategy Map for Security Leaders: People, Processes and Technologies. Retrieved September 13, 2017, from https://securityintelligence.com/a-strategy-map-for-security-leaders-people-processes-and-technologies/

55. Andress, A. (2004). *Surviving security: how to integrate people, process, and technology*. Boca Raton (Fla.): Auerbach Publications. doi:https://books.google.com/books?hl=en&lr=&id=wgs3QL28r64C&oi=fnd&pg=PP1&dq=people process technology for security&ots=49s8JEYaO0&sig=PHFnWl-yyXTTn_G3B4vMeAimoCg#v=onepage&q=people%20process%20technology%20for%20security&f=false

56. Newman, L. H. (2014, April 24). Anonymous Allegedly Hacked Boston Children's Hospital Over Justina Pelletier. Retrieved September 13, 2017, from http://www.slate.com/blogs/future_tense/2014/04/24/anonymous_allegedly_hacked_boston_children_s_hospital_over_justina_pelletier.html

57. Ouellette, P. (2014, September 16). Boston Children's CIO talks DDoS threats, lessons learned. Retrieved July 5, 2017, from https://healthitsecurity.com/news/boston-childrens-cio-talks-ddos-threats-lessons-learned

58. Radichel, T. (2014, August 5). Case-study-critical-controls-prevented-target-breach-35412... Retrieved August 10, 2017, from https://www.coursehero.com/file/16832639/case-study-critical-controls-prevented-target-breach-35412/

59. Kharif, O. (2017, January 19). 2016 Was a Record Year for Data Breaches. Retrieved September 7, 2017, from https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked

60. Swidey, N. (2013, December 16). The Justina Pelletier case: Frustration on all fronts in struggle over child's future - The Boston Globe. Retrieved April 5, 2017, from http://www.bostonglobe.com/metro/2013/12/16/month-medical-ordeal-conclusion-still-uncertain/Y7qvYTGsq8QklkxUZvuUgP/story.html?s_campaign=email_BG_TodaysHeadline

61. Kushner, D. (2017, June 29). How a Crusade to Save Children Landed a Hacker in Prison. Retrieved August 6, 2017, from http://www.rollingstone.com/culture/features/how-a-crusade-to-save-children-landed-a-hacker-in-prison-w489735

59. Eastwood, B. (2014, September 15). How Boston Children's Hospital Hit Back at Anonymous. Retrieved August 30, 2017, from https://www.cio.com/article/2682872/healthcare/how-boston-childrens-hospital-hit-back-at-anonymous.html

60. Gascueña, D. (2016, June 01). Nevil Maskelyne vs Marconi: a Hacker in 1903. Retrieved September 06, 2017, from https://www.bbvaopenmind.com/en/nevil-maskelyne-vs-marconi-a-hacker-in-1903/

61. New, C. (n.d.). Hacking at the Royal Institution. Retrieved October 06, 2017, from http://www.rigb.org/blog/2014/november/hacking-at-the-royal-institution

62. Lord, N. (2017, July 27). The History of Data Breaches. Retrieved September 05, 2017, from https://digitalguardian.com/blog/history-data-breaches

63. Sedova, M. (n.d.). *Carrots not sticks- Using Gamification to Transform Security Mindset of an Organization*. Lecture. Retrieved November 5, 2017.

64. Sedova, M. (2016, July 1). Expanding the Blue Team by Building a Security Culture Program. Retrieved November 16, 2017, from https://www.blackhat.com/us-16/training/expanding-the-blue-team-by-building-a-security-culture-program.htm

65. Lord, N. (2017, July 27). The History of Data Breaches. Retrieved September 05, 2017, from https://digitalguardian.com/blog/history-data-breaches