Fall 2017

CYBERSECURITY IN THE HEALTHCARE ENVIRONMENT

Karla Durham
karla.durham@bhsi.com

CYBERSECURITY IN THE HEALTHCARE ENVIRONMENT

By

Karla A. Durham

Project submitted in partial fulfillment of the

requirements for the

Bachelor of Integrated Studies Degree

Regional Academic Outreach

Murray State University

09/06/2017

FIELD OF STUDY
PROJECT APPROVAL

I hereby recommend that the project prepared under my supervision by

_____,

entitled _____, be

accepted in partial fulfillment of the requirements for the degree of

_____.

_____
Senior Project Faculty Advisor

_____
Departmental Chair

_____
Bachelor of Integrated Studies Advisor

Abstract

In 1990 the online world began to take shape when Tim Berners-Lee invented the World Wide Web. Almost simultaneously, cybersecurity was birthed to protect and minimize the various threats including but not limited to worms, viruses, and data breaches. Cybersecurity includes the various technologies, equipment both hardware and software, processes, and procedures that are used to guard against unauthorized attacks or access to protected information.

This paper will focus on cybersecurity as it relates to the healthcare environment. Every department in a healthcare facility is responsible for taking care of patients. This should be their number one priority and information technology is no exception. While IT staff most likely do not provide hands on care to patients, they go to great lengths to protect their personal health information.

In a healthcare environment, there are numerous departments such as Lab, Radiology, and Pharmacy etc. that need to have integrated systems. These systems must also be able to reach the internet and often be accessible to outside/non-employed vendors for support and maintenance.

Also, communication among employees and with the outside world is a must. Email, video conferencing, desktop sharing, and faxing are all used thousands of times a day. It is imperative that cybersecurity be a top priority and everyone holds himself or herself responsible for protecting the systems that allow staff to take care of their patients.

Table of Contents

INTRODUCTION

Protecting patient information has become a top priority for everyone employed in the healthcare environment. With internet access and state of the art connectivity, the boundaries of healthcare treatments are almost nonexistent and allow for real time responses to patients and their healthcare needs. However, this progression of data sharing and availability comes with a large price tag. Being proactive, planning, and protecting is key to ensuring patients information remains private and secure from attackers.

REGULATORY HEALTHCARE FIRMS

Healthcare information is of extremely sensitive nature and often contains various types of identifiable information such as date of birth, social security number, etc. and must be guarded and protected from improper use. Organizations in the United States who manage healthcare data are regulated by the following requirements:

Health Insurance Portability and Accountability Act (HIPAA) which is a set of federal requirements for protecting patient identifiable health information was instituted in 1996. The two (2) major categories of HIPAA are privacy and security.

The HIPAA Security Rule requires institutions to have policies and procedures in place to protect the confidentiality, integrity, and availability of electronic health information. Confidentiality protects the health information from being disclosed to unauthorized parties, while integrity prevents the information from being stolen, lost, or corrupted. Availability ensures that patient information is readily available to those with a need to know, when needed.

HIPAA security focuses on electronic patient data. Whereas, HIPAA privacy is broader and encompasses all formats of confidential/protected patient information such as paper, oral, and electronic.

The Health Information Technology for Economic and Clinical Health Act (HITECH) and The American Recovery and Reinvestment Act (ARRA) was introduced in 2009. This offered billions of dollars to aid in the development of a national interconnected medical records system. This system gives providers a means to securely exchange patient information and allow patients to access their medical information online. Many are more familiar with the term “meaningful use” which allowed those who adopted an electronic medical record system and met specific criteria by certain dates to receive this special funding.

In March of 2010, the Affordable Care Act (ACA) was presented and provisions were made mandating the sharing of certain types of patient information between healthcare providers and the government. The HIPAA Omnibus Rule introduced protecting personal health information (PHI) among business associates and subcontractors. Penalties for noncompliance with the rule were increased up to a maximum of $1.5 million per violation. Most recently guidelines for mobile health or mHealth were addressed in January 2016. With the ever-increasing population using mobile devices and healthcare providers developing related apps, the US Health and Human Services Department created specific guidelines. Basically, any app or device that works with PHI must comply with HIPAA. (Osterman Research, 2017, pp. 3-4)

SHORTAGE OF CYBERSECURITY EMPLOYEES

Security plans/programs require a robust, skilled workforce. As healthcare facilities transition to electronic health records, cloud based systems, and the Internet of Things (IoT) continues to grow, the amount of information collected and stored grows in astronomical proportions. Unfortunately, the cybersecurity industry has not been able to provide enough professionals to keep up with the demand. Many cybersecurity professionals have their choice of positions in today's job market and employers are unable to hire fast enough.

Report on Patient Privacy (2015) relayed the following:

> The health care industry, with its culture of historically spending less on information security, is at a disadvantage in this competition to attract qualified cyber executives. For example, a 2013 report from the Ponemon Institute found that health care ranked last in its compensation for security professionals, with compensation sited as the No. 1 reason cyber professionals leave their employers. (p.9)

According to Jeff Kauflin, Forbes staff (2017), one of the most in-demand roles is a security analyst who works to mitigate and prevent breaches. In 2012 there were 72,670 security analyst jobs in the U.S., with median earnings of $86,170. Three years later, there were 88,880 such analysts making $90,120. According to a study by analytics firm Burning Glass, cyber security jobs command a $6,500 premium over other IT jobs. A chief information security officer can reach $400,000. (Kauflin, 2017, p. 3).

The healthcare industry saw a 121 percent increase in the demand for cybersecurity employees in the past five years and because of the ever-increasing gap between supply and demand, cybersecurity professionals are able to demand approximately 9 percent higher wages than other IT professionals are. (Landi, 2017).

Certified Information Systems Security Professional (CISSP) is the primary credential in cybersecurity and currently 65,362 professionals hold a CISSP certification. (Landi, 2017). However, this certification takes time, as one must have at least five years of work experience in the cybersecurity field before they can apply for the certification. When compared to the number of job postings there are about three or more job postings for everyone who holds a certificate. In addition, the healthcare industry prefers cybersecurity professionals who also have healthcare skills, financial reporting, and knowledge of HIPAA standards and the HITECH Act. Many institutions report that only half of the staff they employee are adequately trained and qualified when they are hired and state lack of certifications and lack of experience as the causes.

Marc van Zadelhoff of Harvard Business Review feels the following items should be considered when seeking to fill security positions:

- Re-examine your workforce strategy: Do you know what skills you need today and tomorrow to run a successful security program? Realize that skills and experience can come from a variety of places, and adjust your hiring efforts accordingly.

- Improve your engagement and outreach: Don't limit yourself to the same old career fairs and recruiting programs of yesteryear. Get involved in community colleges, P-TECH schools, and other educational programs to start building your recruiting base.
- Build a local cybersecurity ecosystem: Connect with government organizations, educational institutions, and other groups. Sponsor Capture the Flag security events, and work with local middle and high schools to generate interest in the field. These groups are always looking for willing experts and mentors.
- Have a robust support program for new hires: Mentorships, rotational assignments, shadowing, and other opportunities help new cybersecurity hires gain experience and learn. Remember, not everyone knows what they want to do right away. Keep new hires engaged by giving them the creative freedom to work on different projects and explore new technologies and services.
- Focus on continuous learning and upskilling: To retain your new talent, keep employees current on the latest skill sets through classes, certifications, and conferences. Cybersecurity is a highly dynamic field, requiring ongoing education and exploration. And be open to employees from other areas of your business who express interest in cybersecurity career paths.

van Zadelhoff states, "Cybersecurity is a complex career field with extraordinarily challenging problems, but with a diverse pool of experiences and ideas, we stand a much greater chance of successfully defending our assets." (van Zadelhoff, 2017).

FEDERAL GOVERNMENT and HOMELAND SECURITY

According to their website himss.org, Health Information and Management Systems Society (HIMSS) is a not-for-profit association who focuses on better health, and leads efforts to optimize health engagements and care outcomes using information technology (2017). According to Joseph Conn, Modern Healthcare, HIMSS feels the nation could benefit from a national chief information security office. We have had a chief privacy officer for 8 years now. A national cybersecurity leader "would mark a critically important step in elevating the posture of health organizations across the nation," wrote Lee Kim, director of privacy and security at HIMSS. The large amount of patient data that is being breached and the vast amount of internal and external threats are proof this position could be very beneficial. (Conn, 2017)

Most people agree help from the federal government is a must. Alan Webber, lead researcher in the International Data Corp (IDC) 2015 report, *Business Strategy: Defining the U.S. Government Role in Cybersecurity,* believes that government leadership can drive the modernization of technology into the next generation of national cybersecurity. Mr. Webber states, "The size, complexity, and impact of cybersecurity attacks and breaches have grown beyond the size and scope of what the private sector can effectively manage. It has now reached the critical stage where the U.S. federal government has to take a leadership role, in collaboration with businesses and academia, in defining a digital risk response continuum, in shifting our national culture to be more security focused, in establishing a platform for collaborative action and response, and in more effectively supporting research efforts against this modern digital plague." (Webber, 2015).

In May of 2017, President Donald Trump signed a cybersecurity executive order titled “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.” The order was long awaited and most people felt it contained good ideas such as holding agency heads accountable for cybersecurity. However, the senate complained that the U.S. is missing a guiding strategy for cyber defense, more than making adhoc decisions. This was a common complaint during the Obama administration and has continued through to Trump’s group. Many feel the Obama administration made great strides in the cyber arena, but not nearly enough. Unfortunately, the Trump cybersecurity team took a hit in August 2017 when 8 out of 28 members resigned, citing that President Trump is not focusing or placing enough attention on the growing threats of cybersecurity and the affects it has on the critical systems that the American economy depends upon.

According to the 2017 U.S. State and Federal Government Cybersecurity Report, government was ranked 16/18 and healthcare was ranked 13/18 on cybersecurity. For the report, Security Scorecard analyzed more than 500 federal, state, and local government agencies and compared the combined group to 17 other industries on 10 security risk categories: web applications; network security; leaked credentials; hacker chatter; social engineering; exposed administrative portals; Domain Name System health; patching cadence; endpoint security; and malware presence. (Spitzer 2017)

CREATING A SECURITY CULTURE

Does a healthcare organization need a security culture? The answer is absolutely. Security is not a onetime event, but rather a lifestyle that will be forever.

Healthcare organizations should ensure accountability and responsibility for security as part of their core values. Security is embedded in everything an employee does. The threat to information has never been greater. That is why security cannot be optional, but mandatory for all. Everyone has to be responsible for security-whether you are staffing an information desk, sweeping the floors, or working on buildings.

A well-designed security culture is built from the top down. A CEO cannot be exempt and should be responsible for relaying the security message and expectations to all staff. For small walk in clinics or individual physician practices, this might be a smaller feat and easier to accomplish with fewer employees. However, with larger organizations security must be embedded in the culture.

There is still much to learn regarding security and if employees are to think of security as a top priority, they must be educated. There are endless vulnerabilities and they come from everywhere in an organization. A stolen piece of hardware, access to an unauthorized area, eavesdropping, and password sharing are just a few. Security awareness teams are beneficial in driving and reinforcing change that aids in protecting the confidentiality, and availability of both property and information. They accomplish this through awareness and training. Security awareness training must be required at all levels of employment and training should be frequent and ongoing.

Cybersecurity policies, standards, and procedures should be a part of every culture. By setting performance metrics and goals, you can measure and track the effectiveness of the policies against cyber threats to ensure they are adhered to throughout the health care system. Many companies with successful security

awareness programs report they make sure the programs are fun and engaging. They often offer incentives for those who participate. It is also important to make sure employees know to whom they can direct questions. They should feel comfortable to report any/all issues without fear of being reprimanded.

One of the biggest challenges is making employees understand that the choices they make can jeopardize the information they have access to on a daily basis. Most people feel they never place patient information at risk. However, it only takes once.

SOCIAL ENGINEERING

What is social engineering? According to a Norton website one of the more prominent virus protection software companies, it is a way that cybercriminals use human-to-human interaction in order to get the user to divulge sensitive information. Since social engineering is based on human nature and emotional reactions, there are many ways that attackers can try to trick you-online and offline. (Symantec employee, 2017)

Social engineering is a non-technical attack method and is recognized as one of the greatest security threats to healthcare organizations. It does not always involve the exploitation or compromised data for software systems. Attacks often come through emails appealing to urgency, emotions, and pretexting. By playing on a person's emotion, hackers often gain authorized access to PHI and other confidential information with little or no effort. When faced with uncomfortable circumstances or scenarios, people often react quickly and think of consequences later. Cybercriminals count on

human psychology and emotions to gain them access to protected and sensitive information.

One of the most common forms of social engineering is baiting. People have enquiring minds and always want to feel they are “in the know”. Baiting occurs when a device such as a USB flash drive, optical disk, or external drive is left in a common area where it will likely be found. The hacker hopes that curiosity will get the best of the person who finds the device and they connect it to a computer to see the information it contains. If they dangle an item, someone will take the bait. However, once it is loaded/installed a virus or malware activates and allows the attacker access to the victim’s computer system. One should never use a drive or disc that is laying around. It is best to submit it to the local IT or security department to be disposed of properly. Remember you are the first line of defense against social engineering attacks.

Another form of baiting occurs on the web. There are download links, which are really types of malicious software that randomly appear as a person is surfing. The hacker hopes to entice the surfer into clicking on them. They often are lured by a promise of an item or good such as free music, movie downloads, merchandise, or tickets to big games or concerts in exchange for login credentials or personal information. A person should never divulge personal or financial information on an unsecure website nor download files or uncertified applications from an unknown sender. When surfing, beware of links to web forms that request information as well. You should never allow anyone to access your computer remotely. If you encounter a pop up asking you to call a support number while web browsing, close the window immediately. Do not call the number or allow remote sessions over the internet.

Quid Pro Quo is similar to baiting and means and exchange of goods or getting something for something. During this type of social engineering, the end user is promised something for completing a form. Unfortunately, the hacker wants you to include most of your personal information on the form. This information will then assist the attacker in stealing identities.

An attacker may impersonate a person of authority or someone whom you trust to solicit sensitive information. This form of social engineering is called pretexting or bohoing. They make sure it is a role they can play convincingly. For example, they might pretend to be the IT help desk and request your username and password to solve some issue with your computer. They pretend to be someone who would have the right to know in the mind of the victim. In many cases, they just have to have an earnest and authoritative voice and put together a perfect scenario.

Tailgating or piggybacking is another type of social engineering attack and usually encompasses a person desiring access to a restricted item or area. Social engineers can use a variety of tactics. One of the most common examples is for the social engineer to present in a delivery person's uniform carrying a heavy box and ask an authorized employee to open the door for them. Unfortunately, there are staff who assist by allowing them entrance. One should never allow access to a restricted area without the proper identification.

Attackers also try to become a part of large groups that are entering restricted space by becoming one of the group. Staff also have to be aware that people can

mimic other well-known authority figures in a community such as police, technicians, fire marshals, etc.

Social engineers are always playing mind games. They consistently try to control conversations and are very self-confident. They use humor to put their prey at ease and they frequently offer gifts. When they make a request, they usually have a reason such as in the case of the delivery driver who is requesting access to a particular area. It is always important to pay extra attention, especially on a busy day to your work environment.

Have you ever received an unsolicited or unexplained text on your cell phone? If so, you might have been privy to an attack known as SmiShing or SMS phishing. During this type of fraudulent attack a user is duped into downloading a virus or other malware to their cell phone or other mobile device. Victims are often lured into visiting fake websites or returning calls to fraudulent numbers.

Voice over Internet Protocol (VoIP) lets you make a voice call using your internet connection for transmission instead of a traditional analog phone line. While VoIP systems are becoming more affordable and popular in healthcare organizations, by using the same network backbone as your pc, a completely new level of corruption or infection exists. Voice or VoIP phishing is often called vishing. This type of attack is by voice email, voice over IP (VoIP), or landline/cell phone. It's an electronic approach in which people are deceived into providing financial or personal information to unauthorized users. They present as a trusted acquaintance and then try to fish for information by asking you questions to verify your identity.

One of the most well-known cybercrimes is called phishing. Phishing targets can be contacted via email, telephone or text message to obtain items such as credit card information, logins and or passwords. However, many phishing attempts can be upset by recognizing some of the most common characteristics. For example, the email might come from an unsolicited source where the email addresses in the “From” field and “Reply to” persons do not match. It might also be sent in a way to express urgency. One should also be very careful when opening attachments such as *.doc; *.docs; *.rtf; *.pdf; or *.zip files especially if you were not expecting a particular attachment. Many phishing emails contain website links and you can double check and make sure they are legitimate by allowing your icon to hover over the link before clicking. This will allow the web address to appear to ensure the stated link matches the actual website address. Many cyber criminals act in a hurry and often slip up in their email efforts by not catching grammatical errors. They also are not personal in their attempts and use general greetings such as Dear Customer.

If you ever suspect you are on the receiving end of a phishing attack, you should not click on any links, open any attachments, or follow any instructions listed in the email. Always follow the policies or procedures outlined by your organization for reporting suspected phishing attempts and remember a large percentage of breaches start with phishing and they are most effective because the emails appear to have originated from IT administration, health system leaders, or friends/colleagues in need.

Email is one of the greatest tools for communicating both inside and outside an organization. However, there are a number of risks when it is used to transmit or store electronic protected health information (ePHI). Because of these elevated risks,

employees should avoid using email for these reasons if possible. If one must transmit PHI via email, it should be a minimal amount and an email encryption method should be used. Once it has been sent, employees should delete any PHI from their email account and if need be save the information to an approved network location to be used later. Email by default is not encrypted. Therefore, it is important for employees to be aware of the policy and procedure their organization has for emailing PHI. It is also a good practice to password protect any attachments versus including them in the body of an email.

Storing PHI in your inbox, sent items, deleted items, and archives also presents increased risk for potential PHI breaches. Email is one of the first systems targeted when credentials have been compromised and the attacker wants to generate additional phishing attempts. Any PHI data that is still in the compromised mailbox is now available to the criminal. Employees must remember to delete PHI after it has been successfully transmitted per company protocol.

One of the most malicious software attacks to date is known as ransomware. It is designed to block access to a computer system until the demands for a ransom are met. Access is either blocked by locking the screen or locking the users files. The most common form of this malware is crypto-ransomware. This malicious attack encrypts files into coded messages and they can only be decrypted with a key held by the malicious attacker. Ransomware is the prime cyber threat for the healthcare environment and is already costing billions of dollars by inflicting disruptions to operations and cost to organizations to restore these systems. The demand for ransom

monies are frequently paid in a cryptocurrency, which is easily accessible worldwide and is very difficult to trace once the transaction is complete.

Ransomware is one of the most famous attacks. But, it's one of those things, unless you live through an attack it is hard to imagine its affects and the stress that exists for those fighting the battles associated with these attacks. For an organization that is not prepared, ransomware can be devastating.

CYBERSECURITY FRAMEWORKS

Most healthcare organizations begin with a cybersecurity framework for their data security. With systems working towards integrated EHR's and network connected medical equipment, there really is no other option if they are to keep their data secure. While there are several cybersecurity frameworks that have been created, it is not one size fits all. Therefore, it is important for each organization to create their policy/procedures as it relates to data security. Failing to monitor networks appropriately greatly increases the chances of breaches in data.

National Institute of Standards and Technology (NIST) is one of the most common of cybersecurity frameworks. It is a set of guidelines that outline ways organizations with critical infrastructure can align their digital security. NIST was first published in February 2014 and was last updated in January 2017. Various types of organizations have adopted these standards including the healthcare industry.

There are three major components in the NIST: the framework core, the framework profile, and the framework implementation tiers.

The core defines high level activities that companies can participate in to aid in identifying cybersecurity risks, protect against attacks, be alerted when attacks occur, be able to respond to the attacks, and recover from the incident. The framework profiles are often used to describe an organizations current state in regards to security practices. It can also be used to set future goals and objectives. The framework implementation component are tiers that describe specific security processes in levels ranging from partial which is Tier 1 to adaptive which is Tier 4.

The Health Information Trust Alliance (HITRUST) is another common cybersecurity framework. HITRUST is a private company whose framework is a collaborative effort between healthcare/technology and information security leaders.

With the ever-increasing list of requirements with HIPAA, various state and federal regulations, and other industry regulations it is easy to understand why a healthcare organization would seek to be certified by one of these third party vendors. All globally recognized standards are combined in one basic compliance process. The risk of being non-compliant are greatly reduced and organizations are provided with clear guidelines. This is also updated as the healthcare industry changes and regulatory changes go into effect and is designed appropriately to an organizations size and type. Initial standards included ISO, NIST, PCI, and HIPAA to ensure there was a complete list of security controls.

Healthcare systems have to ensure their frameworks are cyber-resilient systems. According to David Ting, co-founder and chief technology officer of The Health Care Industry Cybersecurity Task force relayed there are really five main categories within

building such a system. The first is to identify all vulnerable assets which might include data, systems, infrastructure, or all of these. Second is to develop a strategy for protecting those assets. Managing and controlling who has access and policies around password changes are included in this segment. Detection is third. This is basically understanding when your system is running smoothly or normally and being able to detect when things are not running correctly. The ability to respond and contain an attack or attempt is number four. And finally, if an attack occurs what is the plan to recover. (Spitzer, 2017, p. 57).

SECURING MEDICAL DEVICES

While doing security rounding and even when the security team is completing their risk assessments it is very easy to overlook medical equipment. Often the focus is on laptops, workstations, monitors, etc. However, medical devices can be susceptible to attacks, open to security breaches, and ultimately affect the safety of the equipment. This has become more prominent as biomedical equipment is connected to the internet, hospital networks, and other medical devices. The U.S. Food & Drug Administration allows devices to be placed in the market even though they are open to risk when the benefit to the patient seems to outweigh the risk.

Efforts to minimize cyber threats must be a consolidated effort between the equipment manufacturers and the healthcare organizations who utilize their products to provide patient care. Medical device manufacturers are required to comply with federal regulations. A section of those regulations known as quality system regulations (QSRs) requires manufacturers to identify risks and threats associated with their medical

devices including cybersecurity risks and healthcare facilities are responsible for protecting their hospital systems/networks. Responsibility also extends beyond medical device hardware. The manufacturer is also responsible for testing all software design updates or changes including those that might be required to patch for cybersecurity risk or vulnerabilities. Cybersecurity is not optional for medical devices. It should be a priority in the early or beginning stages of device invention and encompass the lifecycle of the product.

The Medical Device Cybersecurity Act of 2017 (S. 1656) was introduced by Senator Richard Blumenthal from Connecticut on July 27. Blumenthal feels the security of medical devices is in critical condition and that his bill stands to strengthen the healthcare network against the threat of cyberattacks. The bill has currently been read twice, but has already gathered support from two major executive committees, the Association for Executives in Healthcare Information Security (AEHIS) and the College of Healthcare Information Management Executives (CHIME). Blumenthal (2017) stated, “Without this legislation, insecure and easily-exploitable medical devices will continue to put American’s health and confidential personal information at risk.” (Snell, 2017) If this legislation is passed, medical devices will have required cybersecurity testing before the devices are sold.

Cyber-attacks on medical equipment could possibly mean life or death for some patients. Equipment such as MRI machines, ventilators, and IV pumps are often computers. For example, a compromised IV pump or insulin pump could deliver a fatal amount of medication. Whereas, a hacked pacemaker might deliver an unnecessary or deadly shock to a patient. In October 2013 doctors revealed to CNN that they had

ordered the manufacturer to disable the wireless feature on Vice President Chaney's defibrillator in 2007 due to fear that terrorist could hack the device in an effort to assassinate the VP (Ford, 2013). While this scenario sounds as if it came from a TV series, it is actually possible and has been demonstrated.

Sheetal Sood (2017), senior executive compliance officer and head of Information Governance at NYC Health + Hospitals offered the advice below on how to keep healthcare medical devices secure during the National HIPAA Summit in March 2017.

1. **Figure out how these devices connect to the network.** "Do a little classification exercise. Say 'These devices have the most PHI, [so we] classify them as the highest priority', or 'this is the riskiest device as compared to the other ones.'"
2. **Put in some basic controls.** Sood recommends checking to ensure the device isn't using a default password and, if so, changing it to a more secure code.
3. **Lock it away.** Not all security has to be software-based. "If none of the logical controls can be put in, move to some of the physical controls," said Sood. "Lock up the device, put it behind locked doors, or what have you."
4. **Segment the device onto a different network.** "Take all the medical devices and put them on a network that is different from the rest of the organization's network," said Sood. This will keep the devices from being compromised if the rest of the organization is hacked, and vice versa. (Wagenen, 2017)

EMPLOYEE TRAINING

Employees must remember they are the first line of defense for social engineering attacks. It is so important to learn to identify attacks and know how to properly report these attempts to the appropriate personnel. Staff cannot rely on technical safeguards to catch everything. It is everyone's responsibility to protect themselves and their organizations. Data security training is necessary and is required under the HIPAA Security Rule. All covered organizations and business associates must have a security awareness-training program for all members including management.

Training programs should be an ongoing and evolving process. The Office of Civil Rights has suggested computer based training, classroom training, monthly newsletters, posters, email alerts, and team discussions as being beneficial ways to offer security training to employees. HIPAA regulations requires that all training be documented and it is not uncommon during an audit for an investigator to ask for this documentation. The training method, dates and types of training, training materials, and proof of workforce participation should be documented. Cybersecurity training should be part of an employee's initial new hire orientation as well as reviewed annually. There can never be too much education.

Board members are also another group of staff that need to be engaged with the policies and procedures regarding cybersecurity. In January 2017, the National Association of Corporate Directors (NACD) published its updated edition of the

"Director's Handbook on Cyber-Risk Oversight." The publication lists five principles to consider in preparing a cybersecurity training program for board members. (Price, 2017)

1. Cybersecurity is an enterprise-wide risk management issue, not just an IT issue.
2. Understand the legal implications of cybersecurity risks as they relate to a company's specific circumstances.
3. Training should be ongoing, with adequate access to cybersecurity expertise and regular and sufficient time on board meeting agendas.
4. Be clear to your board that members should expect that management will establish an enterprise-wide risk management framework with adequate staffing and budget.
5. Focus training on the identification of which risks to avoid, which to accept and which to mitigate or transfer through insurance.

While education/training will not prevent all cyber-attacks from occurring, it literally can mean life/death for some patients. A good cybersecurity program needs good leadership support, board oversight, and constant attentiveness throughout the organization.

Untrained employees create a massive gap in an organizations inoculation against cyber-criminal activity. It is imperative staff participate and are engaged in their companies cyber defense program. Therefore, it is necessary to educate users on areas of prey such as phishing emails, scams, ransomware infections, etc. It is always best if they can identify these scams or attacks before they make the mistake of clicking

on a link or downloading infectious software. Employees should thoroughly understand what information the hackers are after and how they become a target.

Employees should understand they are responsible for security whether they are actually in the office using their organizations pc or at home accessing links to the office or checking emails from their phone. If employees are using personal tools on an unprotected network, then they are at risk and in turn, they place their place of business at risk.

It is not enough to train employees during their initial orientation and offer a refresher course on a consistent basis. Just as with any other educational experience, the end user should be tested from time to time on the required material. For example, many organizations randomly select employees to periodically receive simulated phishing emails to help them learn to better spot malicious messages. If an employee is targeted with a simulated phishing attempt, security teams remain hopeful they will report it appropriately, delete it from their inbox, and not forward to any other recipients. Unfortunately, some staff are reeled in on these phishing attempts and are frequently offered opportunities to learn more about cybersecurity.

Organizations must remain vigilant with employee training. Employees are truly the biggest reasons for data loss or data being compromised. In May 2016, several Los Angeles county Department of Health Services employees were targeted in a phishing attack. The employees had been trained to recognize and reject phishing email. Even so, 108 of them succumbed to the attack, providing their usernames and passwords. Those compromised workers led to a breach of more than 750,000 records. (Barboza,

2017) This explains why most healthcare organizations are afraid of negligent or careless employee behaviors above all other security threats. It only takes one click to bring down an entire system and cost companies millions in revenue.

HOSPITALS EXECUTING CYBERSECURITY MEASURES

Results from the 2017 AHA Most Wired Survey show that a majority of hospitals are already making the necessary changes to secure information for their patients, physicians, and other providers. Hospitals and care clinics will have to continue making cybersecurity a priority in future years and the AHA has developed various resources to help traverse the various requirements and issues. The Most Wired survey is an annual benchmarking and recognition survey for hospital use of information systems. The 2017 Most Wired survey included data representing 2,158 hospitals, more than 39 percent of all U.S. hospitals.

Most Wired Survey Tracks Hospital Use of Important Cybersecurity Measures

Measure	Share of hospitals implementing measure:		
	More than 90%	More than 80%	More than 70%
Unique identification of system users	✓		
Automatic logoff of system users	✓		
Required use of strong passwords	✓		
Passcodes for mobile devices	✓		
Use of intrusion detection systems	✓		
Encryption of wireless networks	✓		
Encryption of laptops and/or workstations	✓		
Encryption of removable storage media		✓	
Encryption of mobile devices		✓	

Mobile device data wiping	✓		
At least annual risk analysis to identify compliance gaps and security vulnerabilities	✓		
At least annual infrastructure security assessment	✓		
Security incident event management		✓	

Source © 2017 American Hospital Association | July 2017 www.aha.org

One of the most basic requirements in healthcare organizations is to require a unique user identification for access to all electronic information systems that maintain ePHI or proprietary data owned by a particular facility or business partner. User names and passwords for applications are typically assigned by the system administrator and are often associated with a unique enterprise user account. Facilities should also maintain an emergency access procedure or process detailing who is responsible for identifying information in an application that must be accessed in an emergency and who is responsible for creating/maintaining emergency accounts. This type of procedure is often stored in a safe/vault that can be accessed by an approved group of users.

Users should always logoff any and all electronic information systems that maintain ePHI before walking away from their work area. However, there are times in the healthcare environment when emergencies arise and staff have to leave abruptly to respond to a current crisis. Thus, it is common to utilize automatic logoff capabilities when available. Auto logoff times are determined by the criticality and accessibility needs of the computer application. In the event an auto logoff function is not available, employees can quickly lock their computers when away for brief periods. This requires password authentication to log back in. Also many companies utilize a badge proximity

device which allows staff to tap their employee badge on the device to log in and log out of computer equipment quickly and efficiently. This type of setup requires employees to always have their badges with them and it requires employees to report lost or stolen badges immediately. Employees must make every effort to ensure that the confidentiality of access to ePHI is preserved.

Devices and media that contain ePHI are subject to multiple safeguards and password management is one of the most important. It is probably one of the weakest links in an organizations critical line of defense. Therefore, safeguards are put into place as required by the Security Rule and other applicable federal, state, and/or other local laws and regulations. User accounts and passwords should never be shared with anyone. Each organization defines password complexity requirements. However, some of the most common include; Passwords must not contain the users account name or legal name, personal information such as date of birth, names of family members, social security numbers or anything easily guessed by others. Passwords must be a required number of characters in length. Passwords must be different than the previous 10 passwords. Passwords must contain characters from the following:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0-9)
- Special characters (e.g. ?, #, !, etc.)

While it can be frustrating for end users, it is vitally important that passwords be changed frequently. Everyone has forgotten a password at some time. It is important

that employees know who to call or how they can request a password be reset. Some products have the capability of a built-in password reset. Both of these options give employees options and discourage them from the need to write passwords down. Passwords that are written down are regularly left in unsecured locations. Along with password management, it is of utmost importance to make sure that employees have the least amount of permissions required to complete their jobs.

Mobile devices including smartphones, laptops, tablets, portable storage media etc. have presented numerous opportunities for providers when providing patient care when not at the bedside. The flexibility and ease of use make these options very appealing for physicians. However, from a privacy and security standpoint, these mobile tech gadgets bring a completely new set of threats and concerns. They are easy to misplace and are prime targets for theft. Many in the healthcare environment frequently find the need to work away from the office. However, privacy and security policies must always be followed and that responsibility extends beyond the walls of the office. Many organizations are now using software agents such as Airwatch to manage their mobile devices. This allows companies to push software upgrades to the devices and in the event a device is stolen, it allows the company to wipe the device either by specific applications or the entire device.

Many mobile devices do not have strong authentication. Therefore, it is important to take extra steps to secure the device from unauthorized use. Required password protection should be a minimum along with physical control of the device should be maintained. Clinicians most commonly use their mobile devices when they are away from the office and are often in areas where others can view the information

on the device. In these situations, the provider has to remember to take extra precautions so unauthorized viewing of patient information does not occur.

Laptops, tablets, and mobile phones communicate wirelessly. Thus, the wireless connectivity must be protected. Unless a wireless router is secure, it can be reached for quite a distance away, for example several buildings or parking lots away. Wireless should be setup in encrypted mode only. Tools that allow access to a healthcare organizations network have to be designed and implemented with extreme risk avoidance since it is protected by law.

Bring your own device (BYOD) is a concept that is growing as many healthcare organizations face tight budget constraints. However, institutions must develop and maintain policies/procedures to maintain the security of their networks and data. This often includes companies loading proprietary and monitoring software to ensure compliance. A guest or visitors device should never be allowed on a healthcare's production network. Even though it is expensive and consumes the time of IT staff, a guest network is really the best option.

An Intrusion Detection System (IDS) monitors and analyzes network traffic for suspicious and possibly malicious activity or violations and alerts a system or network administrator based upon preset rules. There are various types of IDS with numerous ways of accomplishing the same goal of identifying suspicious or threatening traffic.

A Passive IDS is the most simplistic and truly only detects malicious traffic and simply sends an alert. The receiver is then responsible for any action or blocking of traffic/activity.

A Network Intrusion Detection System (NIDS) is placed at different points within a network and monitors traffic traveling to and from all devices connected to a network. While a Host Intrusion Detection System (HIDS) runs on individual host or devices on a network. This type of detection monitors inbound and outbound packets from a particular device.

An anomaly based IDS uses an established baseline to compare the network traffic. The baseline is what is considered normal such as what ports and devices usually connect and talk, what protocols are acceptable, and what is the typical bandwidth. Alerts are then triggered when activity is detected that differs from the baseline or predetermined factors.

A signature based IDS monitors packets and makes comparisons based on a database that is compiled of signatures from known malicious threats. However, it is imperative the database be kept up to date. Otherwise, your system will not detect new threats leaving your organization vulnerable during this time.

The most advanced IDS is known as Reactive IDS. This intrusion detection system detects and alerts system administrators as well as following pre-defined commands or actions to the threats.

Encryption

Encryption is a common term among IT staff and essentially is a method that converts data into a form that only the intended or authorized parties can understand it. In simple terms, it is protecting data. Unfortunately, it is very easy to access

unencrypted wireless networks. An unencrypted network allows users access to any data saved on the networks computers.

Any healthcare organizations who do not encrypt their devices and data only increase their risk of fines, lawsuits, etc. Patient data typically includes everything a hacker needs to wreak havoc with a person's identity. Stolen patient information can be used to file false medical claims, false tax returns, and even open lines of credit.

Encryption can be a complex subject, but understanding some of the key terms or concepts helps to keep healthcare organizations compliant. The ultimate goal is to protect data where it can only be accessed or obtained by those who are authorized/approved. In the unfortunate circumstances where data becomes available to those who are unauthorized, it should definitely be in a form where it is illegible. This is data encryption.

There are 3 different states or stages of data, at rest, in transit, and in use. Data that is being electronically stored whether on long-term storage or a hard drive is known as data at rest. This includes items such as documents or images. Data being transmitted across a network, sending or receiving is data in transit. An example of data in transit might include transferring a file between computers or using file transfer protocol (FTP) to upload a file to a server. Downloading a file from the internet would also be an example of data in transit. Any data this is temporarily stored within a systems random access memory (RAM) or currently being processed by a computers central processing unit (CPU) would be considered data in use.

Encryption is often referred to in bits such as 128-bit or 256-bit. This number describes the size of the key in bits that is required to decrypt the information. A 128-bit key is equal to 2,128 possible keys and 256-bit equates to 2,256 possible keys. One of the more common encryption methods is Advanced Encryption Standard (AES), which uses 128-bit, 192-bit, and 256-bit encryption. Several cryptographers have attempted to hack through AES, but so far, none has been successful.

According to Peak10's website (2016) reassuringly, 57% of healthcare organizations are using encryption from a third-party, but that leaves over 40% who either haven't adopted encryption yet or are trying to tackle encryption themselves. Some healthcare IT departments have the resources to manage encryption, but many struggle to execute it effectively while keeping up with the other constant demands of technology.

It's not a question of whether your healthcare system will be hacked, but rather will the data they access have any value. Will your organization have to report massive breaches, pay even larger fines, or face irredeemable damages? Encryption minimizes the value to the hacker and often deters them from going deeper into your network/systems and your potential threats are greatly reduced. Encryption is only a small part of a security program. However, having it in place allows healthcare organizations to not have to report breaches if PHI is stolen.

Accessing patient data via wireless devices has become the norm offered by many of our healthcare systems today. Providers and clinicians are being enticed more and more to use the newest technological devices in order to meet government

requirements included in HIPAA and the HITECH Act. Using hand held wireless devices allow physicians to have data immediately available to them while making rounds and they no longer have to carry charts or take the time to sift through stacks of paper. The consensus among most is that mobile devices improve accuracy and therefore, make the providers more efficient. While many healthcare organizations and providers received meaningful use monies by being early adopters of the requirements, they also paid greatly for the advancements in technology.

Most interpret HIPAA to say, any data that is transmitted wirelessly has to be encrypted. This includes devices such as Wi-Fi insulin pumps, glucose monitors, iPads, patient tracking devices, etc. Wi-Fi Protected Access2 (WPA2) is currently one of the most secure methods of encryption available for large organizations. A network utilizing WPA2 requires each client that connects to have their own unique credentials such as a user name/password combination, a token, or acceptance of a certificate.

Full disk, file/folder, and removable media encryption are all used in the healthcare arena. Full disk encryption (FDE) encrypts all data automatically that is stored on a hard drive. Whereas, a user decides which files and or folders are encrypted in a file/folder encryption system.

With theft of patient data on the rise, companies are developing and implementing stringent policies around encryption and the required use of passwords for all mobile devices. Patient information should never be stored or transmitted on an unencrypted device. This includes laptops, USB thumb drives, cellular phones, etc. It

is important for all employees to be knowledgeable regarding the approved methods for data transmission adopted by their organization.

Many healthcare organizations create virtual private networks (VPN) which are safe and encrypted connections that are over less secure networks such as the internet. VPN's were originally designed as a way for users to connect to businesses remotely such as a satellite location needing connectivity back to the corporate office. With a VPN, data travels through secure tunnels and users must use an authentication method to gain access. This type of connectivity is especially beneficial to those employees such as providers or staff who need to work from home or respond when in an on-call status.

Another basic requirement when protecting data against intrusions and threats from outside sources is a firewall. This is a network security device that monitors and allows or disallows traffic both incoming and outgoing on a network based on a selected set of user defined security rules. A firewall can refer to a physical device and/or software that acts as a barrier between trusted versus untrusted sites and networks. In large organizations that use a Local Area Network (LAN), the firewall sits between the LAN and the internet.

BACKUPS

Many feel data backups in any technology environment is part of a basic plan. While backups may be a basic IT function, it is a very critical and vital process that becomes invaluable during a cyber-threat or attack. Identifying and prioritizing sensitive

data according to criticality of doing business is the first step in developing an organizations backup strategy.

However, an excellent backup strategy can prove disastrous if it is not tested. Testing includes not only the backup process, but the restore function. If the data cannot be recovered or restored it is really of no use. It is also important that all backed up information whether it is physical media or a long-term storage device be located off-site. An organization can also benefit from having multiple off-site storage locations.

SECURITY RISK ASSESSMENTS

Healthcare organizations that are committed to ensuring the privacy and security of patient health information as well as ensuring that reasonable safeguards are taken to properly secure patient's ePHI utilize the required HIPAA risk assessment as a primary tool to develop a stronger security environment. A risk assessment should highlight any areas where PHI is at risk as well as confirming compliance with regulations surrounding physical, technical, and administrative safeguards.

Physical safeguards include hardware measures that are in place to aid in the protection of secure electronic patient health information contained in buildings and includes natural and environmental hazards, workstation use, and access controls for the facility and device/media controls. Physical threats might include floods, fire, electrical, earthquakes, etc.

Technical safeguards are not specific requirements, but include technology required to comply with the HIPAA security rules. These safeguards encompass

account access, audit controls, facility access, workstation security and use, and security of transmitted data.

Administrative safeguards include all the procedures and policies that are used to protect and secure ePHI. Security awareness training for employees, business associate agreements, and security incident procedures and planning/evaluation are also a part of administrative safeguards.

Organizations often perform security risk assessments on an annual basis. However, that is not required. It is important to complete a risk assessment when a new EHR is implemented, a new practice opens, or when an existing practice is physically relocated.

When creating a security risk assessment a healthcare organization first needs to define the scope of the risk assessment. Data should then be collected and a list created of all ePHI that is created, where the data is stored, where/how it is received, and transmitted. This may include systems other than the electronic health record and may include 3rd party vendors and websites. This comprehensive list should then be used to review the security measures in place and their effectiveness. This list might include existing safeguards, standards, procedures, processes, controls, and documentation. This is where the technical, administrative, and physical safeguards come into play. It is essential to define the likelihood that a threat would attack an area of vulnerability and to determine the impact if such an incident would occur. This combined determination classifies a risk as high, moderate/medium, or low followed by the prioritization of how the risk is addressed.

Likelihood can be explained as the probability of threat occurrence and can be quantitative or qualitative.

Rating	Likelihood
1	Very low likelihood of occurrence
2	Low likelihood of occurrence
3	Moderate likelihood of occurrence
4	High likelihood of occurrence
5	Very high likelihood of occurrence

Severity or impact is the measure of the effect of a threat. This can be tangible or intangible, qualitative or quantitative. Tangible examples might include replacement cost, lost revenue, monies spent for penalties or settlements, etc. Damage to an organizations reputation or loss of support would be intangible.

Rating	Severity/Impact
1	Threat has minimal or no impact, insignificant
2	Threat has low impact, (minimal effort to resolve)
3	Threat has moderate impact, (limited audience, some effort to resolve)
4	Threat has high impact (Compromise of a large amount of information, loss of reputation/confidence, large system outage)
5	Threat has critical impact (Complete compromise of information, permanent loss, extended outage)

A very low risk rating would mean that a threat could be expected to have minor adverse effects on an organizations operations, assets, staff, other affiliate organization, or might include all of these. Low risk equates to limited adverse effects, moderate risk would have serious adverse effects, high risk equals severe or catastrophic adverse effects, and very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects.

Rating	Overall Risk Rating
1	Very low
2	Low
3	Moderate
4	High
5	Very high

Again, the likelihood rating combined with the impact rating determines the overall risk rating. For example: A likelihood rating of 2 (Low likelihood of threat occurrence) and an impact rating of 4 (threat has high impact on organization) would equal an overall risk rating of 3 (Moderate).

Developing and conducting a security risk assessment can be an overwhelming task. However, healthcare organizations can find free samples or tools on the internet to assist with this daunting task. According to the HealthIT.gov website (2017), the Office of the National Coordinator for Health Information Technology (ONC), the HHS Office for Civil Rights (OCR), and the HHS Office of the General Counsel (OGC)

collaborated and developed a tool called SRA Tool (2017). The tool is free, can be downloaded on various devices, and even has an app for iPad's that can be downloaded from Apple's App Store. The tool contains each HIPAA requirement and consists of 156 questions regarding organizations activities. It also includes resources with each question so that you can review the actual language of the HIPAA security rule, understand the context of the questions, and it helps you to contemplate the influence on PHI if this requirement is not satisfied.

RISK MANAGEMENT

Once a security risk assessment has been completed, it is very important to have a risk management policy/plan in place to address the findings and to be able to effectively communicate the information downstream to all staff. Actually, an organizations risk tolerance should be determined and approved by administration or a governance body prior to the risk assessment. However, once a potential threat is identified or categorized as a risk, it must then be determined how it will be dealt with. For example, if the risk cannot be avoided or is not worth mitigating, organizations may decide to assume or accept the risk. An organization might also decide to discontinue or decommission a device or service known to be causing risk, which in turn avoids the risk all together. However, if a risk cannot be totally circumvented, it can often be minimized and the impact can be lessened to an acceptable level. This is often referred to as mitigation. One other option is transference. This means the liability for a risk is passed along to a third party such as a partner/client or an organization might choose to purchase data breach insurance.

BUSINESS ASSOCIATE AGREEMENT

Healthcare organizations often have other businesses assist with healthcare activities or services and as a result, they disclose protected health information to these third parties or business associates. While the HIPAA Privacy rules applies to covered entities, it allows those organizations to share ePHI on condition that the information is used for the purpose agreed upon with the covered entity and so long as the business associate safeguards it from misuse. Business Associate Agreements must be in writing. The United States Department of Health and Human Services provides us with the following examples (2017).

Examples of Business Associates.

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan’s pharmacist network.

If a data breach or violation occurs with the business associate, the covered entity is required to resolve the breach or end the violation. If this cannot be completed successfully, the contract/agreement should be terminated. If for some reason the contract cannot be terminated the covered organization is required to report the issue to the HHS or OCR.

VIRUS PROTECTION

Anti-virus software protection is another requirement high on this list in order to combat the unwanted threats in the cybersecurity arena. It is not enough just to install virus software, but it must be kept up to date with the latest virus definitions and patches to protect against malware. In large organizations these tasks are usually completed by the Information Technology Department. Fortunately, virus software is easily available, reliable, and financially affordable.

Healthcare organizations should make sure they have policy and procedures in place requiring the use of anti-virus software on all computers including mobile devices and handhelds. It is also important that staff be knowledgeable regarding the common symptoms of viruses or malware in case their device becomes infected. According to the article “Top 10 tips for Cybersecurity in Health Care” (2017) on the Healthit.gov website, symptoms of an infected computer might include:

- System will not start normally (e.g., “bluescreen of death”)
- System repeatedly crashes for no obvious reason
- Internet browser goes to unwanted web pages
- Anti-virus software does not appear to be working

- Many unwanted advertisements pop up on the screen
- The user cannot control the mouse/pointer

MULTIFACTOR AUTHENTICATION

Many healthcare organizations are adding an additional layer of authentication to their systems in an effort to tighten security and further protect their data. It is commonly referred to as multifactor or dual authentication. In addition to a unique user ID and password, users are prompted for additional information in order to obtain access. Unfortunately, logins and passwords are often compromised whether they are guessed, stolen, or hacked and additional authentication to verify ones identity enhances the security of your account even if your password has been compromised.

There are numerous multifactor authentication technologies including security tokens for instance, smart cards or key fobs, soft tokens such as PINS or approval request transmitted to an additional device for example a smart phone, and even biometric authentication methods including fingerprint scans, voice recognition, and facial recognition.

THE HIGH COST OF CYBERCRIME

Chuck Spurr, Chief Information Officer with Shields Health Care Group summed up the latest in security challenges facing Healthcare. “It used to be that data in the healthcare world was the second tier [for hackers]. People weren’t going after it. Now people are going after it a lot harder and faster. They no longer just want the social security number. It is the entire medical record they really want. Now you have to protect yourself completely. Now, we are moving into telemedicine and other things and

we are expanding all of our tools. So as we expand our tools out we are expanding our footprints and risk, and that really gets very difficult. So it is much more complicated than it was five years ago." (Spurr, 2017)

According to a report by Ponemon Institute and Accenture the average cost for a cybercrime is $11.7 million per business globally in 2017. The report also states healthcare companies spend an average of $12.47 million on cybercrime-related expenses each year with healthcare being the fifth most costly industry. (Cohen, 2017)

Stolen medical records are a big win to cybercriminals and contain a wealth of information. According to Mariya Yao, Women@Forbes the going rate on the black market for a social security number is 10 cents and a credit card number is worth 25 cents, but an electronic health record can be worth hundreds or even thousands of dollars. (Yao, 2017) It is easy to report a stolen social security card or credit card and request a new card and number. However, your information contained in your medical record once exposed cannot be retracted and in the hands of criminals can prove destructive for one's entire life.

A medical record contains your demographic information such as address, phone number, age, social security number, place of employment, contact information for relatives and next of kin, insurance/financial information, past and current medical history, problems, medications, test results, etc. It is truly a living document and a person's identity.

In 2016, the cyber world was hit with a ransomware attack known as Petya. It was truly an attempt by the hackers to receive financial gain by demanding a ransom.

Petya was programmed to infect the master boot system of computers running Windows based operating systems, causing the data in the hard drives file system to become encrypted and prevent the pc from booting. A ransom message would then appear on the screen stating the user could receive a decryption key and have their system restored if they would pay the ransom being demanded via Bitcoin. It was reported that some organizations had some success once the ransom was paid with decrypting their files.

In June 2017 many healthcare giants fell victim to a global attack that caused destruction and devastation to many industries in its path. It was originally thought to be Petya. However, researchers have learned that hackers used ransomware as a mask to cover their real intent, which was the disruption and destruction of data. This has since been called NotPetya ransomware. NotPetya affects systems in the same way as Petya. However, it does not allow the user any opportunity to obtain/enter a decryption key or an opportunity for file restoration.

Merck's, a giant pharmaceutical company reported the Petya cyberattack costing them $135 million in revenue. Their incomes were drastically reduced due to temporary production shutdown, higher demand than planned, and lost sales in certain markets due to the virus. (Davis, 2017)

Nuance Communications, a dictation and transcription service for physicians experienced wide spread outage in June 2017 that continued for several weeks due to Petya. According to fast facts on the Nuance website, they transcribe more than 7 billion lines of medical data annually, more than 10,000 hospitals in the US. utilize

Nuance healthcare solutions, and more than 150,000 doctors and caregivers use the Dragon Medical application (2017). It is almost impossible to measure the loss from such a massive interruption in services. Fortunately, Nuance did not have to report a data breach, but rather a security incident according to the HIPAA Security Rule.

However, many healthcare and related organizations were not so fortunate in 2017 and cybersecurity criminals along with their own employees required them to be public with reportable data breaches.

While not quite as famous as ransomwares WannaCry and Petya/NotPetya, there is another group of hackers responsible for their own version of ransomware called The Dark Overlord. Unfortunately, this group is running rampant among smaller healthcare clinics in the United States and costing millions. On January 11, 2017, they hacked a server and back-up drive of Cancer Services of East Central Indiana-Little Red Door demanding 50 bitcoin ($43,000) in ransom. The request for ransom first began as text messages to the executive team including the director, president, and vice president but was soon followed by letters and emails. While the company stood firm and refused to pay the ransom, they also lost their data and are being forced to replace hardware and rebuild all the stolen data. They have since made the decision to transition to a cloud-based system (Davis, 2017)

Indiana Medicaid mailed notification letters to patients upon learning there were medical records that were exposed as early as February 2017. This was the result of a report containing medical information being easily accessible via a hyperlink on the internet. The report included patient's names, their Medicaid ID number, name and

demographic information of the physician, patient number, procedure codes, dates of service and the amount paid by Medicaid to the providers. While many think this information will not be used improperly, a patient's privacy has been violated (Sullivan, 2017).

Molina Healthcare, a major Medicaid and Affordable Care Act insurer was required to shut down a patient portal after an anonymous tip unveiled a security flaw that allowed users access to other patient's medical claims data without necessitating authentication. A user simply had to change one number in the web URL to obtain this access. Unfortunately, this breach exposed patient names, demographic information, diagnosis, and medications, all of which are easily used for fraud. The exact number of patient records compromised was not released. However, Molina Healthcare serves 4.8 million customers in 12 states and Puerto Rico and all patient records appeared to be affected (Davis, 2017).

Many healthcare organizations use cloud storage or third party vendors to backup and store their information. However, that option too, has its vulnerabilities. Bronx-Lebanon Hospital Center in New York utilizes iHealth Innovations based in Louisville, Kentucky for records storage. Unfortunately, on May 3, 2017 a leak was discovered that was produced by a misconfigured Rsync backup server, the results of a hack by a third party. NBC News reviewed records and reported the breach revealed a patients' mental health and medical diagnoses, HIV statuses, sexual assault, and domestic violence reports along with names, addresses, addiction histories, and religious affiliations (O'Hara, 2017).

It is very difficult to fathom or identify all patient information that has been criminally mined and how it will be used. A hacker who identifies as Skyscraper confided to DataBreaches.net that there are approximately 500,000 records belonging to children that are available for purchase on the dark web. He even stated that simple searches for “patient” could return entire databases that have been left exposed. According to James Scott, Senior Fellow with the Institute for Critical Infrastructure Technology, children’s records are in high demand on the dark web. A September report from ICIT conveyed depending upon how much information is included and the market type a complete medical record is worth $500 to $1,200 on the dark web. A criminal can build a fake identity from this information and not be discovered for a very long time (Davis, 2017).

While there is a large amount of focus on cybercriminal activity, theft of equipment containing patient data is also on the rise. In January 2017, Denton Heart Group reported a stolen unencrypted hard drive containing 7 years of backup EHR data. While in April, Washington State University also reported an unencrypted hard drive with the potential of affecting 1 million people.

While the cost to protect your healthcare organization from cyber-criminal activity seems unaffordable, it only takes one breach of patient information and any savings and any additional monies will be lost. In the healthcare industry, employees owe it to their patients to take care of their medical, spiritual, and emotional well-being, as well as protecting all personal information.

Conclusion

There is no question that cybercrimes are rising and healthcare organizations with their wealth of patient information are prime targets for this costly criminal activity. It is no longer a question of whether or not your company will be targeted; it is just a matter of when. Preventing immediate access to patients medical records or compromised or hacked medical equipment could easily mean life or death for some patients. The damages whether financially or to an organizations reputation, will be determined by the preparations that have been made beforehand.

It is extremely important healthcare organizations make security a top priority from the executive suite and board members to the bottom position on the organizational chart. Securing patients demographic, personal, and medical data is everyone's responsibility. A security culture must exist and all employees must be engaged.

There are many items that are vitally important such as firewalls, encryption, password policies, backups, risk assessment, pen test, etc. However, breaches that occur in the healthcare environment are predominantly associated with staff who have been spoofed or hacked. Nothing is more significant than the training of staff. It is so important that healthcare organizations teach, guide, and protect. Employees should always be aware, know the warning signs of malicious activity, and be knowledgeable on how to report questionable concerns without fear of retribution.

Being proactive, planning, and protecting remain the main keys to ensuring patients information remains private and confidential.

References

American Hospital Association, (2017, July). Hospitals implementing cybersecurity measures. [PDF document] Retrieved November 12, 2017, from http://www.aha.org/content/16/factsheet-cybersecurity.pdf

Barboza, T., (2016, December 17). L.A. County targeted in phishing cyberattack; private information of 750,000 people compromised. *Los Angeles Times*. Retrieved from http://www.latimes.com/local/lanow/la-me-ln-county-cyberattack-20161217-story.html

Cohen, J., (2017, October 2). Cybercrime costs healthcare companies $12.5M per year, report finds. Retrieved October 31, 2017, from https://www.beckershospitalreview.com/cybersecurity/cybercrime-costs-healthcare-companies-12-5m-per-year-report-finds.html

Conn, J., (2016, November 15). HIMSS says federal government needs a national chief information security officer. Retrieved September 19, 2017, from http://www.modernhealthcare.com/article/20161115/NEWS/161119958

Davis, J., (2017, January 19). Indiana Cancer Agency hacked by TheDarkOverlord. Retrieved November 4, 2017, from http://www.healthcareitnews.com/news/indiana-cancer-agency-hacked-thedarkoverlord

Davis, J., (2017, May 3). Hacker: Patient data of 500,000 children stolen from pediatricians. Retrieved November 4, 2017, from

http://www.healthcareitnews.com/news/hacker-patient-data-500000-children-stolen-pediatricians

Davis, J., (2017, May 30). Molina Healthcare breached, exposed patient data for over a month. Retrieved November 4, 2017, from http://www.healthcareitnews.com/news/molina-healthcare-breached-exposed-patient-data-over-month

Davis, J., (2017, October 27). Petya cyberattack cost Merck #135 million in revenue. Retrieved October 31, 2017, from http://www.healthcareitnews.com/news/petya-cyberattack-cost-merck-135-million-revenue

Ford, D., (2013, October 24). Cheney's defibrillator was modified to prevent hacking. Retrieved October 21, 2017 from http://www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html

Health Care Compliance Association (2015, September). [PDF] Privacy/Cybersecurity Industry Faces Growing Worker Shortage. *Report on Patient Privacy, 15*(9), 9. Retrieved from http://www.hcca-info.org/Portals/0/PDFs/Resources/Rpt_Privacy/2015/rpp0915.pdf

Health Information and Management Systems Society (HIMSS), (2017). Retrieved September 19, 2017, from www.himss.org

HealthIT.gov, (2017). Top 10 tips for cybersecurity in health care., Retrieved October 21, 2017, from https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

HealthIT.gov, (2017). What is the Security Risk Assessment Tool (SRA Tool)? Retrieved October 18, 2017, from https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

Kauflin, J., (2017, March 16). The Fast-Growing Job With A Huge Skills Gap: Cyber Security. Retrieved September 9, 2017, from https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#2938ed565163

Landi, H., (2015, October 28). Healthcare Industry Faces Shortage in Experienced Cybersecurity Experts. Retrieved November 9, 2017, from https://www.healthcare-informatics.com/news-item/healthcare-industry-faces-shortage-experienced-cybersecurity-experts

Norton (2017)., What is social engineering? Retrieved September 21, 2017, from https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

Nuance., (2017). *Making technology more human*. [Fact Sheet]. Retrieved October 31, 2017 from https://www.nuance.com/about-us/fast-facts.html

O'Hara, M., (2017, May 10). Thousands of patient records leaked in New York hospital data breach. Retrieved from https://www.nbcnews.com/news/us-news/thousands-patient-records-leaked-hospital-data-breach-n756981

Peak10, (2016, July 8). Healthcare, encryption and HIPAA compliant systems: How they're connected, why they're crucial. Retrieved October 6, 2017, from

http://www.peak10.com/healthcare-encryption-hipaa-compliant-systems-how-theyre-connected-why-theyre-crucial/

Price N., (2017, September 11). Training hospital board members about cybersecurity threats. [Web log comment]. Retrieved from http://www.boardeffect.com/blog/training-hospital-board-members-cybersecurity-threats/

Quest (2017). Protecting data in the healthcare Industry. [White Paper]. Retrieved November 9, 2017, from https://www.quest.com/whitepaper/protecting-data-in-the-healthcare-industry8128353/

Snell, E., (2017, August 15). Medical device cybersecurity top challenge to IoT ecosystem. Retrieved September 5, 2017, from https://healthitsecurity.com/news/medical-device-cybersecurity-top-challenge-to-iot-ecosystem

Spitzer, J., (2017, August). 5 questions with Imprivata CTO David Ting on healthcare's cybersecurity problem. *Becker's Hospital Review*, *2017, No. 8*, 57.

Spitzer, J., (2017, August 24). How 18 industries rank on cybersecurity. Retrieved November 9, 2017, from https://www.beckershospitalreview.com/cybersecurity/how-18-industries-rank-on-cybersecurity.html

Spurr, C., (2017). *HIMSS 17 In focus. All in: Embracing cybersecurity across the healthcare enterprise.* [PowerPoint Slides]. Retrieved November 4, 2017, from http://www.healthcareitnews.com/himss-infocus/cybersecurity?

Sullivan, T., (2017, July 5). Indiana Medicaid warns patients of health data breach. Retrieved November 4, 2017, from http://www.healthcareitnews.com/news/indiana-medicaid-warns-patients-health-data-breach

U.S. Department of Health & Human Services, (2017)., Business Associates. Retrieved November 4, 2017, from https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

van Zadelhoff, M., (2017, May 4). Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It. Retrieved November 9, 2017, from https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

Wagenen, J., (2017, March 31). National HIPAA Summit: 4 steps to better securing medical equipment. Retrieved October 21, 2017, from https://healthtechmagazine.net/article/2017/03/national-hipaa-summit-4-steps-better-securing-medical-equipment

Webber, A., (2015, July). Business Stragegy: Defining the U.S. Government Role in Cybersecurity. Doc# GI1257300. Retrieved November 9, 2017, from https://www.idc.com/getdoc.jsp?containerId=GI257300

Yao, M., (2017, April 14) Your electronic medical records could be worth $1000 to hackers. Retrieved October 31, 2017, from https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#1faceb150cf1