Spring 2017

An Examination of Modern Challenges in Maintaining HIPAA and HITECH Compliance

Andrew Miller
University of North Georgia, asmill0296@ung.edu

An Examination of Modern Challenges In Maintaining HIPAA and HITECH Compliance

A Thesis Submitted to
The Faculty of the University of North Georgia
In Partial Fulfillment
Of the Requirements for the Degree
Bachelor of Business Administration in Information Systems
With Honors

Andrew S. Miller
Fall 2016

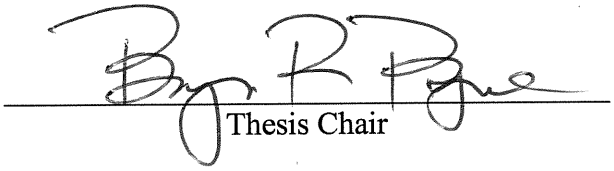
Accepted by the Honors Faculty

of the University of North Georgia

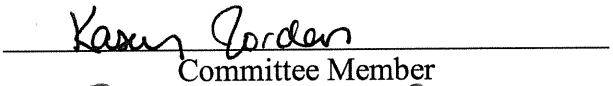
in partial fulfillment of the requirements for the title of

Honors Program Graduate

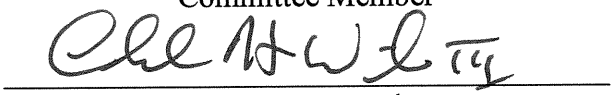
Thesis Committee:



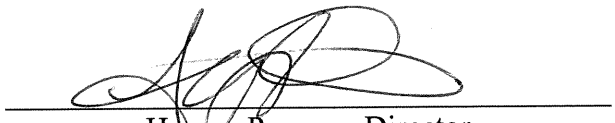
Thesis Chair



Committee Member



Committee Member



Honors Program Director

Acknowledgements

This thesis would not have been possible without the assistance and encouragement from many people. I am truly grateful for the help I received from many people, and I would like to express my thanks to each of them.

First, I would like to thank Dr. Stephen Smith and the University of North Georgia (UNG) Honors Program for the support and guidance I was given throughout my project. Dr. Smith provided valuable feedback on various aspects of the process, and was an excellent help in the selection of the thesis committee members. In addition, I would like to thank Corey McCown and Cole Edgar of UNG Information Security for their help in locating information about current threats facing enterprises. Dr. Joanne Patterson of UNG Nursing and Angela Megaw of UNG Libraries both provided excellent assistance in locating information about healthcare science.

In addition, I had the support of an excellent thesis committee. Dr. Charles "Trey" Wilson was able to serve with his legal background, and Kasey Jordan was able to serve with her nursing background. Both of these members showed extreme amounts of support for this project, and I thank them for their willingness to be on this committee.

Lastly, I would like to extend a huge thank you to Dr. Bryson Payne of the UNG Computer Science department. Dr. Payne provided hours of his time while he served as the thesis committee chair of this thesis project. He worked with me on almost all aspects of the project, and I owe a great deal of the success to him.

Abstract

This paper will discuss the challenges modern healthcare providers face in maintaining full compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Acts. It will provide an overview of the pertinent sections of both the HIPAA and HITECH Acts. Further, the paper will discuss potential large-scale violations of HIPAA involving potential vulnerabilities in commonly-used enterprise health records systems. In addition, the paper will discuss the traditional weak points of information security, including: people susceptible to social engineering, software that cannot be or is not updated, and targeted attacks. It will then compare these to challenges to the challenges of the United States health system prior to 1995, specifically looking at information handling procedures, and how they have changed as relating to the effectiveness.

Introduction

Technology's use in the developed world has increased exponentially since the Industrial Revolution[1], and healthcare is no exception to this trend. An early example of this technology is the ophthalmoscope, which came about in the 1840s and subsequently improved by a group of scientists.[2] The ophthalmoscope is used to assist medical professionals in performing examination of animal eyes, and is notable for the innovative

---

[1] Robert U. Ayres. 1989. Technological transformations and long waves. Part II. Technological Forecasting and Social Change 37, 2 (February 1989), 111–137. DOI:http://dx.doi.org.libproxy.ung.edu/10.1016/0040-1625(90)90065-4

[2] Franklin M. Lusby ed. 2015. Ophthalmoscopy. (February 2015). Retrieved June 5, 2016 from https://www-nlm-nih-gov.libproxy.ung.edu/medlineplus/ency/article/003881.htm

use of magnification through mirrors to give medical professionals a clear and enlarged view of the eye.[3]

Shortly after the invention of the ophthalmoscope, numerous other advances came along, including: the x-ray, the stethoscope, the laryngoscope, and many other technological instruments.[4] These instruments empowered medical professionals to become more equipped to perform their job, all the while decreasing the need for surgery for many less severe, common health ailments, using medical imaging technology.[5]

Shortly after the Second World War, innovators introduced computer information systems to the healthcare field. This allowed for past medical history to be accessed through a terminal and later a computer at speeds previously impossible with paper files in the facilities with this technology. An attempt to standardize the exchange of this information and to make it easily interchangeable amongst healthcare providers in the state was made by the Massachusetts General Hospital in 1966.[6] This effort led to the production of the programming language MUMPS, which stands for Massachusetts General Hospital Utility Multi-Programming System.[7] MUMPS is still widely used in modern health information systems, including EPIC Systems[8], GE Healthcare[9], Quest Diagnostics[10], and many others.

---

[3] Ibid.
[4] Irvine Loudon. 1997. Western Medicine: An Illustrated History, Oxford University Press.
[5] Ibid.
[6] Keith Snell. M21. Retrieved June 5, 2016 from http://www.m21.uk.com/newtom.php
[7] Ibid.
[8] Zina Moukheiber. 2013. Behind Epic Systems, A Low-Key Health IT Company Called InterSystems. (March 2013). Retrieved June 5, 2016 from http://www.forbes.com/sites/zinamoukheiber/2013/03/04/behind-epic-systems-a-low-key-health-it-company-called-intersystems/#e8b207b4ac10
[9] Luis Ibanez. 2012. Join the M Revolution. (February 2012). Retrieved June 5, 2016 from https://opensource.com/health/12/2/join-m-revolution
[10] William Vorhies. 2016. MUMPS – The Most Important Database You (Probably) Never Heard Of. (January 2016). Retrieved June 5, 2016 from http://www.datasciencecentral.com/profiles/blogs/mumps-the-most-important-database-you-probably-never-heard-of

HIPAA Introduction

While each advance in technology brought its own challenges, all of these paramount technological advances served and continue to serve an important purpose: to advance science and improve healthcare. However, it became apparent that with the growing role of healthcare information technology in the United States, that there was significant information being collected by such technological systems. This information was subject to potential abuse or mishandling from healthcare workers, as well as being compromised by malicious hackers. Further, before 1996 CE, the United States federal government possessed little power in terms of healthcare regulations[11], leaving the vast majority of the power to individual states in terms of governance of standards.

In addition to potentially causing misunderstandings with proper information handling from out-of-state or travelling health professionals, the lack of uniform health data governance led to issues with insurance policy differences between states, medical coding differences, fraud, and many other issues.[12] These differences in governance led to increased healthcare costs, increased health insurance cost, and may have contributed to sensitive patient information being disclosed improperly by first and third parties due to the lack of unifying, national privacy set of laws.[13]

The United States Congress set out to address the issues with the lack of uniform health information data handling standards. In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to address said concerns.[14] In

[11] John J. Trinckes. 2013. The definitive guide to complying with the HIPAA/HITECH privacy and security rules, Boca Raton, FL: CRC Press.
[12] Ibid.
[13] Ibid.
[14] Ibid.

addition to establishing clear standards for the conditions of health data disclosure by healthcare providers, it also established standards for: information security, patient privacy, fraud prevention, electronic data exchanges, healthcare access, revenue, and insurance standardization.[15]

HITECH Act Introduction

In the decade after Congress passed HIPAA, there was a rapid growth in healthcare demand, caused by an aging population, an increase in population, and other factors.[16] This placed a strain on the capacity of health environments to accurately keep track of the patient data, and to have a way to securely transmit and disclose the information. In addition, there was a recession that began in the United States in 2007[17] which severely limited the budget of many healthcare providers, leading to hiring freezes, discretionary spending cuts, customers unable to pay their bills, and reduced spatial expansion of healthcare facilities.[18]

The United States congressional bodies recognized the challenges caused by the increased demand and shrinking budgets, and set out to have hearings about it. These hearings featured many differing viewpoints from medical and IT professionals.[19]

Despite the differences of opinion expressed at the HITECH Act's hearing, there was a general consensus that further health information reform was needed. Unlike the

---

[15] June M. Sullivan. 2004. HIPAA: a practical guide to the privacy and security of health data, Chicago, IL: American Bar Association, Health Law Section.
[16] Lindsay M. Howden and Julie A. Meyer. 2011. Age and Sex Composition: 2010. US Government Census Data (March 2011), 2.
[17] Anon. 2009. Crisis and recovery, Washington, D.C.: International Monetary Fund.
[18] Anon. 2009. National Survey of Family Doctors Shows Recession Takes Startling Toll on Patients. (May 2009). Retrieved June 6, 2016 from http://www.aafp.org/media-center/releases-statements/all/2009/nationalsurvey-familydoctors-recession.html
[19] Anon. 2010. Hearing Before the Subcommittee on Health of the Committee on Energy and Commerce. (2010), 32.

previous HIPAA guidelines, which did not mandate electronic records in most instances, the HITECH Act set a deadline of 2015 before penalties would be imposed upon health providers who are not using electronic health records.[20] The lawmakers realized this endeavor would cost the health field a significant amount of money, so they included grants to offset the cost of migrating to an enterprise health records system.[21] This added the HITECH Act to the American Reinvestment and Recovery Act of 2009 (ARRA), as this provided an unprecedented amount of funding to assist eligible providers in funding the initiatives set forth in the HITECH Act.[22]

Additionally, the HITECH Act set relatively strict guidelines for the data handling, insisting that the data be used meaningfully by eligible providers.[23] Assuming the providers met the requirements, struggling facilities utilized tremendous cost savings that are associated with storing records electronically.[24]

Data Breach History

Prior to widespread electronic health record usage, most breaches of information and trust in the healthcare environment primarily occurred on a small scale through more primitive attack methods. These methods included methods that primarily relied on abusing human trust, such as social engineering, shoulder surfing, using misplaced documents, and breaking into record rooms.[25]

---

[20] Joy Dark and Jean Andrews. 2012. CompTIA healthcare IT technician HIT-001 authorized cert guide, Indianapolis, IN: Pearson.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Lawrence O. Gostin and Joan Turek-Brezina. 1995. Privacy and security of health information in the emerging health care system. Health Matrix: Journal of Law-Medicine 5, 1 (January 1995), 1–36.

The next section of this paper contains numerous examples of how health data can be compromised. It is important to note that this serves in no way as an extensive list of breaches, and that breaches can occur in many ways.

One of the most common method used by attackers to gain sensitive medical information prior to the passage of HIPAA was social engineering.[26] There were many ways this took place. For example, if there was a high-profile local figure in a health environment, a media employee or contractor may attempt to gain information about the figure by going to the health environment they are in and posing as a grieving family member. The employee could then ask for as much information as they were able to, and given the lack of established protocol, they were often able to get the room number the figure was in, the condition for which they were actively being treated, and their medical history. With this information, the media employee now is able to publish the information before other agencies, motivated by bringing fame and curious viewers to their media entity.

However, the motives of social engineers were often more sinister than abusing sensitive information for a news agency. An example of such would be in cities where gang activity is rampant, and gang leaders would do all they could to destroy their rival gangs. In this instance, a gang member may be in a hospital setting with an undisclosed ailment. A gang member in a rival gang may hear of this, and possibly wants to murder the gang member in the hospital while bed-ridden and defenseless.

For the gang member to do this, he may go to the hospital posing as a religious minister, and asks to see the patient who happens to be in a rival gang. He could then go

---

[26] Ibid.

and says a few words of encouragement to the gang member, and could provide the information of location to another one of his own gang members, who may go straight to the room posing as a doctor. While under the cover as doctor, he could clear the room, and has the ability to poison the patient's water and food supply, take clothing, bodily samples, or other belongings to be used to frame the patient for crimes, shoot the patient in the hospital, or any number of other things.[27]

With the passage of HIPAA, patients have a right to know the directory information that will be provided to guests of the facility, as well as redact the information in a fashion the patient sees fit. A person at high risk for their data being compromised by nefarious parties would have prevented the above hypothetical situation from transpiring by employing these safeguards.[28]

Shoulder-surfing and eavesdropping techniques were also frequently used in the healthcare environment prior to the passage of HIPAA.[29] To shoulder-surf, an individual would stand near a medical professional, and look over their shoulder to view patient information, including: medical records, social security numbers, insurance and financial information, and other classified information.[30] Similarly, an eavesdropper would be within earshot of departments where patient data is collected or dispersed, such as registration, the emergency department, or billing.[31]

To counteract this potential for sensitive information to be compromised, HIPAA mandates that privacy be maintained through necessary measures, including privacy

---

[27] H.Dominic Covvey and Neil H. McAlister. 1980. Computer-assisted medicine: privacy and security. Canadian Medical Association Journal 123, 3 (August 1980).
[28] Anon. 2003. Summary of the HIPAA privacy rule HIPAA compliance assistance, Washington, D.C.: U.S. Dept. of Health and Human Services.
[29] Covvey. 1980. Computer-Assisted.
[30] Ibid.
[31] Ibid.

screens where needed and not having boards such as the emergency department's patient triage board visible to people other than those with an immediate connection to the department.[32] These measures make it drastically more difficult for an unauthorized person to obtain this information.

Prior to the passage of HIPAA, health record storage practices had not yet achieved standardization in the United States.[33] It was not uncommon in many health environments to have a patient's medical records sitting on a counter beside registration, containing the patient's: social security number, street address, phone number, marital status, insurance information, billing information, medical history, and other sensitive information.[34] This was taken advantage of by individuals of nefarious intent, including: identity thieves, insurance fraudsters, sexual predators, house robbers, and other criminals.[35]

Perhaps the greatest possibility of a large-scale health record breach would be a compromise of the physical security of a data records room, allowing an attacker to gain unrestricted access to the records of a health institution's patients. This would provide a far larger avenue for information to be compromised, provided the attackers were able to pose as employees with legitimate purpose to be in the room interacting with records, such as a nurse or medical coder.

While there is not reliable data available on attackers compromising a records room and making off with physical health records prior to 1996, the HHS Office of Civil

---

[32] Anon. 2003. HIPAA.
[33] Ibid.
[34] D. Irvine. 1994. Confidentiality: data and permissible disclosure. Journal Of The Royal Society Of Medicine 82, 22 (1994), 42–43.
[35] Ibid.

Rights (OCR) has collected such information since the passage of HIPAA. Since 1996, there have been over 400 recorded breaches of health information that were from paper health records.[36] This works out to around 40 breaches per year, and is skewed towards having more than 40 per year prior to 2010, due to the passage of the HITECH Act and organizations transitioning away from paper records. The largest recorded breach of paper records involved 483,063 individual records in 2016.[37] In total, the OCR has recorded over 2,400,000 individual paper records being breached from 1996 CE – 2016 CE.[38]

Modern Threats

While the modern healthcare providers face new and challenging problems each day, such as drug-resistant bacteria, emerging diseases, legal changes, and so on, the information security departments that work with these facilities faces new threats every day, which can be just as deadly as any of the aforementioned healthcare problems.

One such threat could be a terroristic threat involving placing a payload on the interface engine that is set to distort the data sent between departments. The interface engine is usually found in larger hospitals, and is an internal device that is responsible for allowing communication of Health Level 7 data between the appropriate electronic medical record systems. The interface engine is not needed in smaller facilities, as they often use a single electronic medical record system to store patient information, as opposed to a large enterprise network of electronic medical record systems that different departments use.

---

[36] Anon. Breaches Affecting 500 or More Individuals. Retrieved September 10, 2016 from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[37] Ibid.
[38] Ibid.

With the attack on the interface engine, an attacker would first need to gain control of the system as outlined in the following "Proof of Concept" section. Once the attacker has gained control, they will simply need to adjust the code that is responsible for converting the data for each system. Due to the fact that the system will do what the code tells it to do, the code can say anything, including targeted attacks for assassinations and untargeted attacks for terroristic reasons.

An example of an assassination that could be committed by taking control of an interface engine would be a simple conditional statement that is only set true to the target's personal identifying information, such as their medical record number, name, address, phone number, emergency contact, social security number, etc. Anything could be placed inside the conditional statement. For example, if the attacker wished to subject the target to intense pain and suffering, the attacker may have the conditional statement report that the results from the lab's electronic medical record system that are being sent to any other system be placed into a switch statement. The switch statement could have sections for the type of test, as well as the result of the test, and what to change them to before being sent further. For example, if the target had a culture performed on something suspicious the target had in their body at the lab that was benign, the switch statement may change it to something invasive. To further increase the suffering of the target, the attacker may also prevent any allergy information (the AL1 field[39]) from being transmitted to or from any of the record systems, thus allowing doctors and pharmacies to provide the targeted patient with doses of medicines and treatments that they are allergic to.

[39] Joel Rodrigues. 2010. Health information systems: concepts, methodologies, tools and applications, Hershey PA: Medical Information Science Reference.

Likewise, the switch statement could do things such as remove actual diagnostic results, and replace them with all clear results indicating that the patient is fine when they may in fact be dying quickly and in need of immediate treatment and care. In addition, the patient may have a treatment that is easily treated with something that the target is not allergic to, but not easily treated with something else. For example, the target may have contracted a disease such as syphilis that is easily treatable with antibiotics in most instances. However, the switch statement could have the lab results of the resistance analysis of the strain removed from the patient show strong resistance to every antibiotic except the tetracycline class of antibiotics. The switch statement could then have the patient's allergy information show that they are allergic to the tetracycline class of antibiotics, which could prevent the target from getting access to the proper treatment, and may instead have the patient develop neurosyphilis and die an agonizing slow death.

That said, it would be quite possible to have an attacker perform an untargeted terroristic attack on patients in a hospital in the same way, only all or random patients would be affected, as opposed to only selected patients. This could be done with political motivation, financial motivation, or other terroristic motives.

More frequently, hackers are not looking to harm or kill people. They are instead looking to steal their health records, and then resell them on the "black market". Health records are significantly more valuable than other information, such as financial information. Recently, 10 Medicare numbers were for sale on one such website for approximately $4700, or around $470 per account.[40] This is significantly larger than the

[40] Aarti Shahani. 2015. The Black Market For Stolen Health Care Data. (February 2015). Retrieved September 10, 2016 from http://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data

often-quoted value of $50.00 per record on the black market, and the value is likely to increase further as time progresses.[41]

The largest healthcare information breach recorded by the HHS Office for Civil Rights occurred with a similar motive, albeit on a much larger scale. On March 15th, 2015, analysts discovered that hackers had exploited a vulnerability in the connection between Anthem Incorporated and the users of this company.[42] It is estimated that over 78,800,000 individual records were taken by hackers from this breach.[43] This is an extreme case of why business associate agreements are required for the use of healthcare data; without strong agreements, all 37 of Anthem's clients would be legally responsible for Anthem's breach, as opposed to Anthem.[44] On this note, any organization using off-site technology for health record storage or analysis should have a strong business associate agreement established.

However, attacks on hospital IT infrastructure could occur on any system, and are not limited to critical systems such as the discussed attacks on providers' systems. Further, attacks can have any motive, and are not limited by any factor whatsoever. This is why the securing of every single system that is connected in any way to the healthcare facilities network is crucial to ensuring that all patients get the timely and professional care from the healthcare workers.

For example, in the Target data breach in which hackers took over 40,000,000 credit card numbers, the analysts discovered that the hackers had entered the network

---

[41] Ibid.
[42] Joseph Conn. 2015. Legal liabilities in recent data breach extend far beyond @AnthemInc. (February 2015). Retrieved September 10, 2016 from http://www.modernhealthcare.com/article/20150223/news/302239977
[43] Ibid.
[44] Ibid.

through a computer that was running a Linux distribution[45]. The computer system was for Target's HVAC vendor, and the company left all passwords default on it.[46] Target allowed the company to have the system open for remote access to monitor and control the HVAC system as needed. The system was in no way secured, or segregated from the internal Target network, despite Target's internal information security team being aware of all of this.[47]

While the example of the Target breach is not directly related to the proper information handling procedures of health information technology, it does illustrate that a system as innocent-in-appearance as the HVAC computer can be the breach that costs over $100,000,000 in direct damages, and possibly billions in indirect damages when costs such as issuing new cards, refunding fraudulent purchases, etc. are accounted for.[48]

However, it would be feasible for a breach similar to Target's to occur in a healthcare environment. There are many specialized devices on a hospital network with direct links to either the interface engine or the health information system. For this reason, network segmentation is not always a feasible approach to ensuring that patient data remains secure. In cases like this, it is critical that the devices are being closely monitored, and that they have all security patches run regularly on them.

Unfortunately, there are a significant amount of these devices no longer receiving any security updates on networks in healthcare facilities. For example, Billy Rios and Mike Ahmadi recently discovered that versions 8.0 through 9.3 of the Pyxis

---

[45] Brian Krebs. 2015. Inside Target Corp., Days After 2013 Breach. (September 2015). Retrieved August 11, 2016 from http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/
[46] Ibid.
[47] Ibid.
[48] Ibid.

SupplyStation software have over 1400 vulnerabilities.[49] Of these vulnerabilities, the US Department of Homeland security scores 715 of the detected vulnerabilities with a CVSS score from 7.0 to 10.0.[50] This is the highest score given, and many of these are relating to vulnerabilities that can be exploited remotely.[51]

To further complicate matters, Microsoft has recently estimated that 17.9% of online systems will come in contact with malware in 2016[52], and Symantec has 4,156,033[53] individual virus signatures in its virus definitions as of August 11th, 2016. For the healthcare industry, this can caused be everything from slowing a computer in the registration office, to stopping the operation of the life support machines in the critical condition facilities.

For example, an employee in the registration department may have visited a site that was recently compromised by malware, or may even have visited a honeypot of a common misspelling of legitimate website, and downloaded and installed a keylogging application on a production registration computer. A honeypot is a system or website that appears legitimate, but is actually used for hacking or research purposes, such as a malicious website on gogle.com. Assuming the keylogger operates at startup, has the appropriate permissions provided it, is not detected by the antivirus program(s) employed by the facility, and is available to all users of the computer, the employee and others then

---

[49] Zeljka Zorz. 2016. 1,400+ vulnerabilities found in automated medical supply system. (April 2016). Retrieved September 10, 2016 from https://www.helpnetsecurity.com/2016/03/30/1400-flaws-automated-medical-supply-system/

[50] Anon. 2016. CareFusion Pyxis SupplyStation System Vulnerabilities. (March 2016). Retrieved September 10, 2016 from https://ics-cert.us-cert.gov/advisories/icsma-16-089-01

[51] Ibid.

[52] Anon. 2016. Microsoft Security Intelligence Report (SIR). (January 2016). Retrieved August 11, 2016 from https://www.microsoft.com/security/sir/default.aspx

[53] Anon. 2016. August 11, 2016 Rapid Release Definitions - Detections Added. (August 2016). Retrieved August 11, 2016 from https://www.symantec.com/security_response/definitions/rapidrelease/detail.jsp?relid=2016-08-11

input their usernames and passwords into the various programs that they use to record registration, billing, and other information about the patients, which is recorded by the keylogger. Additionally, any information typed by the employee using the infected machine is subject to this recording, including: patient's full names, phone numbers, dates of birth, social security numbers, medical history, insurance information, etc. With this valuable information, the hacker can either use the information themselves, or more commonly can sell this information on black market exchanges in exchange for bitcoins, or any other currency medium that is not easily tracked.

However, information is not the only resource that healthcare facilities have. Almost every healthcare facility in the developed world has a powerful, high-speed network and many powerful nodes on it. An attacker may want to use some of this potential to perform nefarious acts, such as distribute illegal content, perform distributed denial of service attacks on websites, send spam email, etc. utilizing these resources. The attacker may then add certain nodes on the facility's network to a botnet, which is a collection of computer that work together to accomplish goals set by a central authority, which is usually a hacker.

Luckily, botnets at current tend to produce traffic patterns that are easily recognizable by commercial firewalls that are almost certainly deployed by facilities of all sizes. This attack medium would not generally be successful in the long term for that reason.[54] However, in smaller facilities, this is a real threat that may overtake the network and all machines if not properly monitored and prevented.

---

[54] Anon. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2 - Configuring the Botnet Traffic Filter [Cisco ASA 5500-X Series Firewalls]. Retrieved August 12, 2016 from http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_botnet.html

Apart from this, there are countless other types of malware capable of wreaking havoc on networks in healthcare environments in ways similar to the described attacks, such as viruses, worms, Trojan horses, etc. To remain in compliance with the HITECH Act and to maintain information security and integrity as outlined in HIPAA, it is extremely important that all healthcare facilities place great emphasis on safeguarding all aspects of data, which requires a constant and conscientious effort by all employees, contractors, and associates of the facility to achieve.[55]

Proof of Concept

In reality, it is relatively easy for a dedicated hacker to access and take control of aspects of a network. Tools are widely available on the internet to aid in this task, as well as to demonstrate where the vulnerabilities are in implementations of employed solutions, such as network, system, software, etc. Additionally, there are a growing number of websites and videos online that teach prospective hackers how to best utilize the available tools, many of which are freely available without payment for personal use.

At this point, it is important to emphasize that these tools can be used by "black hat hackers" or "white hat hackers." The main difference between the black and white hats is the motive; white hat hackers generally are doing penetration testing that they are directly authorized by the sole owner or other party with the authority to do so of the system that they are testing to verify that they are or are not able to breach the established safeguards and defenses of that which they are attempting to compromise.[56] Black hat

---

[55] Anon. 2015. $750,000 HIPAA settlement underscores the need for organization-wide risk analysis. (December 2015). Retrieved August 12, 2016 from http://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html

[56] David M. Hafele. 2004. Three Different Shades of Ethical Hacking: Black, White, and Gray. (February 2004). Retrieved August 12, 2016 from https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390

hackers are generally motivated by another factor, such as stealing property, fame, terrorism, or other criminal motives.

However, white hat and black hats also generally act differently in how they react to compromising. A white hat may get in and plant a "dummy payload," which proves that penetration is possible without disrupting actual operations, whereas a black hat may plant a malicious payload, which not only proves that penetration is possible, but then disrupts operation and allows the hacker a large amount of control over the network.

One of the most popular tools available for this purpose is actually a compilation of tools. Kali Linux is a freely available Linux distribution based on Debian, which includes a plethora of tools for testing and penetration of networks, software, and other devices. Kali Linux has been downloaded over 1,000,000 times[57], and is used extensively by both white and black hat hackers.

One of the things that Kali prides itself on is being relatively easy to use. Compared to other solutions, Kali is free to download, and will run on most x86 machines made in recent years. In addition, Kali is loaded with a plethora of utilities that are usable right after installation, that allow everything from password cracking, network scanning, to social engineering attacks.

To demonstrate this, all that is needed is a bootable Kali flashdrive and a computer capable of running 64-bit software. This flashdrive is easily made by first downloading the latest Kali Linux iso from a reputable distributor, and verifying the SHA1sum of the file with the provided information on the Kali Linux downloads page.[58]

---

[57] Mati Aharoni. 2015. Kali Moto End of Life & Kali Dojo Slides. (October 2015). Retrieved August 11, 2016 from https://www.kali.org/news/kali-moto-eol/

[58] Raphaël Hertzog. Kali Linux Downloads. Retrieved August 12, 2016 from https://www.kali.org/downloads/

The purpose of verifying the SHA1sum of the download is to ensure that the iso file has not been compromised by either corrupted files or man-in-the-middle attacks, and can be done using a variety of programs on modern operating systems. Once the file has been downloaded and verified for integrity, it simply needs to be copied to a freshly formatted flashdrive using either a terminal command such as “dd” or an application capable of copying iso images to external media that allows them to be bootable devices.

Once the bootable device has been made, it simply needs to be inserted into the appropriate port of the computer, and selected to be booted from in the device boot options upon startup of the computer. At this point, several options will appear for boot options. Depending on how permanent the hacker wishes the installation to be, they will either select the option for live boot, in which the operating system will be loaded on the memory of the computer in a temporary fashion, or the installation option, in which Kali’s system files are transferred and installed on the computer’s solid state or hard drive.

With Kali running, the hacker will do a series of things, but for this example will open the Metasploit program in Kali Linux for the first time. Metasploit will open a terminal window in which the program is initialized and loaded, as well as the database of exploits it contains. Once Metasploit is fully loaded, in this example, the hacker types “Armitage” and hits the enter key. Armitage, which a powerful graphical user interface that allows novice hackers to use Metasploit with ease, will then load. From this point, the hacker will either import a previously scanned nmap scan using the import hosts option, or perform an nmap scan from the Armitage window. Nmap scans are used to

determine what devices are on a specified IP address or range of addresses, as well as which ports are open and services are running on said devices.

With the hosts imported, the hacker will then select the option to find attacks. This will test each exploit in the database to see if it is able to run, and is highly dependent upon the updates run on the system, the open ports, the antivirus program, the firewall, and the packages installed. From there, the hacker will simply right click on the machine in the Armitage window, select an exploit, and run it. It will either allow the hacker in or not, and if it does not, the hacker simply tries until they gain access. Once they have access, they can do a variety of things, depending upon the type of machine, but will typically monitor the network internally, create administrator accounts, install spyware, etc.

It is important to note that in the previous example, the hacker already had the IP address of the machine that they wished to access. This is not always the case when hacking, however, it is generally not difficult to locate the IP address of a network. For example, an attacker could get a public address of the webserver by simply visiting the website of the hospital. Social engineering could be used on any employee in the building by simply calling, asking to speak with a name found in a public directory, asking them to run a command such as "ipconfig /all" in command prompt, and having the employee read off the applicable information.[59] In addition, the attacker could simply go to the facility, locate an Ethernet port, connect a machine to it, and then locate the IP address.

It is also important to note that the previous example used very basic steps for hacking, and that it will not always be limited to the above steps. For example, if the

[59] Mindi McDowell. 2009. Avoiding Social Engineering and Phishing Attacks. (October 2009). Retrieved August 11, 2016 from https://www.us-cert.gov/ncas/tips/st04-014

attacker wished to change the content on a webserver running Linux and MySQL, they may simply use a program such as Burp Suite in Kali Linux to test for SQL injection vulnerabilities. There are many types of systems in many locations for many purposes, and an almost infinite amount of ways to compromise them.

Security

Despite the ease that hackers experience when accessing many systems, it is an achievable task to ensure that hackers are not able to access systems without the proper authorization. Although every health organization is unique, the following will prevent most attacks from being successful: keeping all software up-to-date, running an enterprise antivirus on all applicable machines, employing network security, educating and training employees on information security risks, encrypting all sensitive files and communication with secure algorithms, enforcing a strong password policy, and limiting access by access groups.

The importance of patching is evidenced by the 2016 Enterprise Security Report that Hewlett Packard recently released. In this report, they determined that 68% of exploits used in 2015 that they analyzed were provided patches over two years ago.[60] These old, patched exploits very likely would not have been able to have been used by hackers on the enterprise systems to attack them had their system administration team been adamant about patching software in a timely and responsible fashion.

The same report by Hewlett Packard illustrates the following amount of new malware discovery increases by platform in 2015 from the previous year: Microsoft

---

[60] Sue Barsamian. 2016. The collateral damage of cybercrime. (2016). Retrieved August 12, 2016 from http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

Windows, 88%; Google Android, 153%; Linux, 212%; Apple iOS, 235%.[61] For this reason, having a strong, enterprise class antivirus program that blocks malware from being loaded on systems is important to the healthcare field, and it is crucial that regular scanning be done to verify that systems remain clean.

The need for strong network security is well-evidenced in the aforementioned example of Target's data breach. Had they not allowed remote access, and segmented their network, the attackers very likely would have been able to recover over 40,000,000 card numbers from the corporate network.

For the healthcare environment, given the regulations that employees are expected to be in full compliance with at all times through HIPAA, HITECH, and other legislation, it is crucial that they be trained on information handling principles, such as avoiding phishing scams, social engineering, and malware threats. This is accomplished through training and having skilled information security experts available to answer questions at all hours of operation, and will have a varying but generally positive outcome on the information security of enterprise environments.[62]

Even with the best technological safeguards, it is still possible that a zero-day exploit can allow a hacker unauthorized access to a healthcare system's network. For this reason, it is imperative that sensitive information be encrypted using the best algorithms available, such as the Advanced Encryption Standard. With AES, the hacker will not

---

[61] Ibid.

[62] Michael Sanchez. 2011. 5 Ways to Educate Employees about Network Security. (May 2011). Retrieved August 12, 2016 from http://blogs.cisco.com/smallbusiness/5-ways-to-educate-employees-about-network-security

receive files that are easily usable, and will instead need to use advanced hardware for a long time that at this point is not generally feasible for individuals to have.[63]

However, even with firewalls and other network security devices fully up-to-date, it would still be relatively easy for a hacker to access the network using a user's insecure or repeated password. For example, it is estimated that approximately 1/3 of users use the same password on every website[64], meaning that if a hacker hacks a site and finds a user's login information, they are then able to use that login information to access the healthcare's network approximately 1/3 times. For this reason, it is generally best to have passwords expire after a set amount of days, such as 90, and to not allow users to repeat previous passwords. Additionally, to allow for a much larger pool of possible combinations of characters, it is best to set strong complexity and length requirements, as for each additional character, there can be millions more combinations.[65]

One of the most important aspects of maintaining compliance is to do so with meaningful use, and one of the easiest ways to accomplish this is through utilizing access groups by position. Tools such as Microsoft's Active Directory make this task easy, and through Active Directory Federation Services, it is easy to use this information across a multitude of platforms, including keycards for accessing restricted areas.

Comparison and Contrasting Storage Mediums and Closing Arguments

Compared to previous record storage methods, information is far easier to be leaked without authorization. That said, with a vigilant staff who work together to protect

---

[63] Anon. 1998. Cracking DES: secrets of encryption research, wiretap politics & chip design, San Francisco, CA: Electronic Frontier Foundation.

[64] Flavio Martins. 2014. 3 Quick Facts on Why a Strong Password Policy Matters. (May 2014). Retrieved August 12, 2016 from https://blog.digicert.com/3-reasons-for-strong-password-policy/

[65] Ibid.

all information, it is an achievable goal to remain in full compliance with HIPAA. For example, while it was previously possible to break and enter the records room, it was not easy to do so without detection. It was also not feasible to take an entire hospital's records and hold them hostage, as is possible with ransomware.

However, with the proper safeguards outlined, it is entirely possible and obtainable for organizations of all sizes to prevent unauthorized entry of electronic records, as well as to mitigate damages from attacks using the preventative measures outlined in this paper.

Works Cited

Aarti Shahani. 2015. The Black Market For Stolen Health Care Data. (February 2015). Retrieved September 10, 2016 from http://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data

Anon. 1998. *Cracking DES: secrets of encryption research, wiretap politics & chip design*, San Francisco, CA: Electronic Frontier Foundation.

Anon. 2003. *Summary of the HIPAA privacy rule HIPAA compliance assistance*, Washington, D.C.: U.S. Dept. of Health and Human Services.

Anon. 2009. *Crisis and recovery*, Washington, D.C.: International Monetary Fund.

Anon. 2009. National Survey of Family Doctors Shows Recession Takes Startling Toll on Patients. (May 2009). Retrieved June 6, 2016 from http://www.aafp.org/media-center/releases-statements/all/2009/nationalsurvey-familydoctors-recession.html

Anon. 2010. Hearing Before the Subcommittee on Health of the Committee on Energy and Commerce. (2010), 32.

Anon. 2015. $750,000 HIPAA settlement underscores the need for organization-wide risk analysis. (December 2015). Retrieved August 12, 2016 from http://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html

Anon. 2016. August 11, 2016 Rapid Release Definitions - Detections Added. (August 2016). Retrieved August 11, 2016 from https://www.symantec.com/security_response/definitions/rapidrelease/detail.jsp?relid=2016-08-11

Anon. 2016. CareFusion Pyxis SupplyStation System Vulnerabilities. (March 2016). Retrieved September 10, 2016 from https://ics-cert.us-cert.gov/advisories/icsma-16-089-01

Anon. 2016. Microsoft Security Intelligence Report (SIR). (January 2016). Retrieved August 11, 2016 from https://www.microsoft.com/security/sir/default.aspx

Anon. Breaches Affecting 500 or More Individuals. Retrieved September 10, 2016 from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Anon. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2 - Configuring the Botnet Traffic Filter [Cisco ASA 5500-X Series Firewalls]. Retrieved August 12, 2016 from http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_botnet.html

Brian Krebs. 2015. Inside Target Corp., Days After 2013 Breach. (September 2015). Retrieved August 11, 2016 from http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

D. Irvine. 1994. Confidentiality: data and permissible disclosure. *Journal Of The Royal Society Of Medicine* 82, 22 (1994), 42–43.

David M. Hafele. 2004. Three Different Shades of Ethical Hacking: Black, White, and Gray. (February 2004). Retrieved August 12, 2016 from https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390

Flavio Martins. 2014. 3 Quick Facts on Why a Strong Password Policy Matters. (May 2014). Retrieved August 12, 2016 from https://blog.digicert.com/3-reasons-for-strong-password-policy/

Franklin M. Lusby ed. 2015. Ophthalmoscopy. (February 2015). Retrieved June 5, 2016 from https://www.nlm.nih.gov/medlineplus/ency/article/003881.htm

H.Dominic Covvey and Neil H. McAlister. 1980. Computer-assisted medicine: privacy and security. *Canadian Medical Association Journal* 123, 3 (August 1980).

Irvine Loudon. 1997. *Western Medicine: An Illustrated History*, Oxford University Press.

Joel Rodrigues. 2010. Health information systems: concepts, methodologies, tools and applications, Hershey PA: Medical Information Science Reference.

John J. Trinckes. 2013. *The definitive guide to complying with the HIPAA/HITECH privacy and security rules*, Boca Raton, FL: CRC Press.

Joy Dark and Jean Andrews. 2012. *CompTIA healthcare IT technician HIT-001 authorized cert guide*, Indianapolis, IN: Pearson.

June M. Sullivan. 2004. *HIPAA: a practical guide to the privacy and security of health data*, Chicago, IL: American Bar Association, Health Law Section.

Keith Snell. M21. Retrieved June 5, 2016 from http://www.m21.uk.com/newtom.php

Lawrence O. Gostin and Joan Turek-Brezina. 1995. Privacy and security of health information in the emerging health care system. *Health Matrix: Journal of Law-Medicine* 5, 1 (January 1995), 1–36.

Lindsay M. Howden and Julie A. Meyer. 2011. Age and Sex Composition: 2010. *US Government Census Data* (March 2011), 2.

Luis Ibanez. 2012. Join the M Revolution. (February 2012). Retrieved June 5, 2016 from https://opensource.com/health/12/2/join-m-revolution

Mati Aharoni. 2015. Kali Moto End of Life & Kali Dojo Slides. (October 2015). Retrieved August 11, 2016 from https://www.kali.org/news/kali-moto-eol/

Michael Sanchez. 2011. 5 Ways to Educate Employees about Network Security. (May 2011). Retrieved August 12, 2016 from http://blogs.cisco.com/smallbusiness/5-ways-to-educate-employees-about-network-security

Mindi McDowell. 2009. Avoiding Social Engineering and Phishing Attacks. (October 2009). Retrieved August 11, 2016 from https://www.us-cert.gov/ncas/tips/ST04-014

Raphaël Hertzog. Kali Linux Downloads. Retrieved August 12, 2016 from https://www.kali.org/downloads/

Robert U. Ayres. 1989. Technological transformations and long waves. Part II. *Technological Forecasting and Social Change* 37, 2 (February 1989), 111–137. DOI:http://dx.doi.org/10.1016/0040-1625(90)90065-4

Sue Barsamian. 2016. The collateral damage of cybercrime. (2016). Retrieved August 12, 2016 from http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

William Vorhies. 2016. MUMPS – The Most Important Database You (Probably) Never Heard Of. (January 2016). Retrieved June 5, 2016 from http://www.datasciencecentral.com/profiles/blogs/mumps-the-most-important-database-you-probably-never-heard-of

Zeljka Zorz. 2016. 1,400+ vulnerabilities found in automated medical supply system. (April 2016). Retrieved September 10, 2016 from https://www.helpnetsecurity.com/2016/03/30/1400-flaws-automated-medical-supply-system/

Zina Moukheiber. 2013. Behind Epic Systems, A Low-Key Health IT Company Called InterSystems. (March 2013). Retrieved June 5, 2016 from http://www.forbes.com/sites/zinamoukheiber/2013/03/04/behind-epic-systems-a-low-key-health-it-company-called-intersystems/#e8b207b4ac10