WORLD LIBRARIES

Volume 24

No. 1

2020 worldlibraries.dom.edu/index.php/worldlib |

Cybersecurity Threats in Healthcare Organizations: Exposing Vulnerabilities in the Healthcare Information Infrastructure

Seth Evangelista Hoffman

Dominican University

ABSTRACT

The healthcare industry has been brought to the limelight with the recent COVID19 pandemic. Everyday, the world waited for information from various data warehouses to report positive cases as well as effective treatment processes that help direct patient care. It was in 2009 that the HITECH Act was passed to promote and expand the adoption of health information technology, by converting paper records into computerized or electronic records to improve quality and safety of care through efficient, and timely exchange of information between the patient and the members of the healthcare team. Today, 30% of the world's data belong to the healthcare industry. As healthcare data exponentially increase, so does the security and privacy threats to consumer's personal and medical information. Both government and private advocacy agencies have created policies and standards to safeguard the public against cybercrimes. But what is imperative is transparency among healthcare organizations in exposing the potential vulnerabilities in their technology infrastructure so that collaborative strategies are created to address these cybersecurity threats. The Anthem security breach is provided as an example to identify weaknesses in healthcare organizations. Recommendations for healthcare organizations are provided as well as the role of consumers in the prevention of cybercrimes in healthcare is discussed.

***Keywords**: cybersecurity; healthcare; health information technology; electronic health records; cybercriminals; threats in healthcare*

INTRODUCTION

Background

The United States Department of Health & Human Services (DHHS), also known as the Health Department, is a part of the executive branch department of the U.S. Federal government. The DHHS is in charge of programs that deal with protecting the health of all Americans by providing essential health services. President Obama, as a part of Obamacare, through the DHHS established the HITECH Act, under the direction of the Office of the National Coordinator (HealthIT.gov, 2019).

The HITECH Act or Health Information Technology for Economic and Clinical Health Act is part of an economic stimulus package included under American Recovery and Reinvestment Act of 2009 (ARRA). The goal of the HITECH Act a way to promote and expand the adoption of health information technology, by converting patient's paper medical records into computerized or electronic records. The use of electronic health records aims to improve the efficiency and timeliness of data exchange between consumers and their providers, among the members of the healthcare team, between health-related organizations throughout the continuum of care and insurance companies (HealthIT.gov, 2019).

The HITECH Act, also updated the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and implemented safeguards to keep health information private and confidential, restricting uses and disclosures of health information. The HIPAA Privacy Rule describes what information is protected and how protected information can be used, disclosed and to whom. The HIPAA Security Rule describes who is covered by the HIPAA privacy protection and what safeguards must be in place to ensure appropriate protection of electronic protected health information (HealthIT.gov, 2019).

Health.gov (2019) states that the Cures Act was established to improve the flow and exchange of electronic health information, including the delivery of information, advancing interoperability, prohibiting information blocking, and enhancing the usability, accessibility, and privacy and security of health IT. ONC works to ensure that all individuals, their families and their health care providers (researchers, drug companies, collaborating agencies) have appropriate access to electronic health information to help improve the overall health of the nation's population.

Figure 1 shows how (this author) Seth a student athlete at DU shared his electronic health record with several providers within the continuum of care. In 2019 Seth broke his arm while at Dominican University. His Coach took him to the Rush University Medical Center Emergency Department. His demographic information, medical history, insurance information as well as all the test results during that visit was entered and stored into an electronic health record within Rush University's EHR's system. This includes the X ray result of his arm. After the season was over, Seth requested a copy of that X-ray result to be sent to his Orthopedic surgeon in Las Vegas so he can get evaluated and start therapy. After the summer was over another X-ray was done by his Las Vegas ortho to check whether the fracture was healed and an evaluation was dictated to clear him to play baseball. Instead of option for his records to be sent electronically to DU he opted to have them printed out and given to him personally. He also went to a Quick Care in Las Vegas to see a physician for a physical exam and a specific DU form to be filled out. He personally uploaded all these hard copies into his personal computer, converted them into PDF files and uploaded them into the DU Athletic Department website.

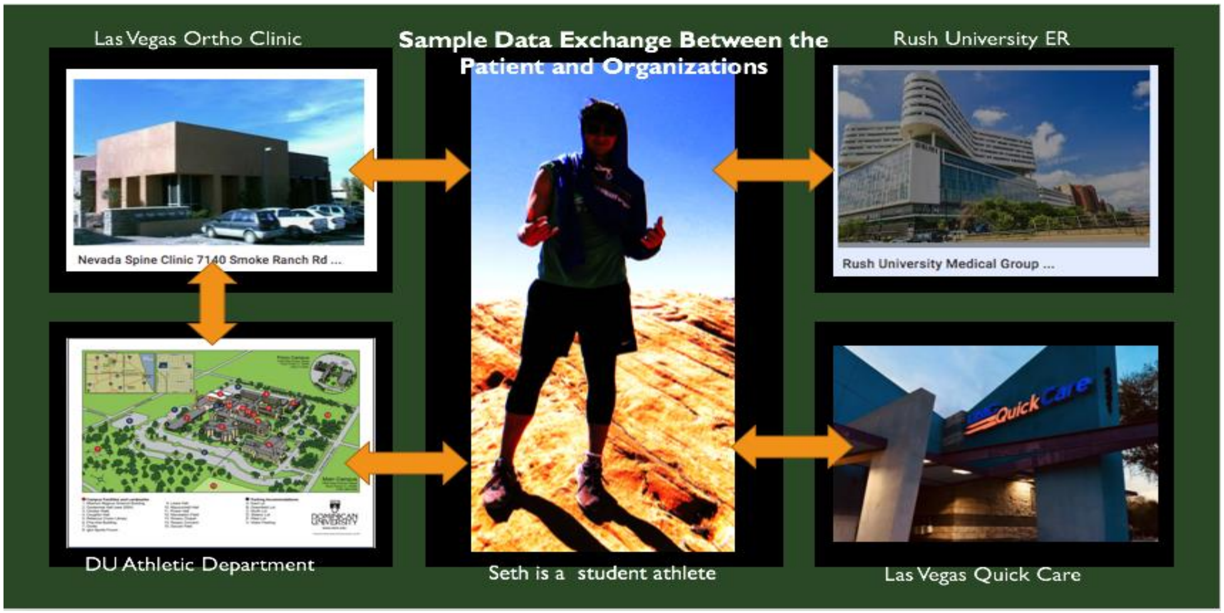
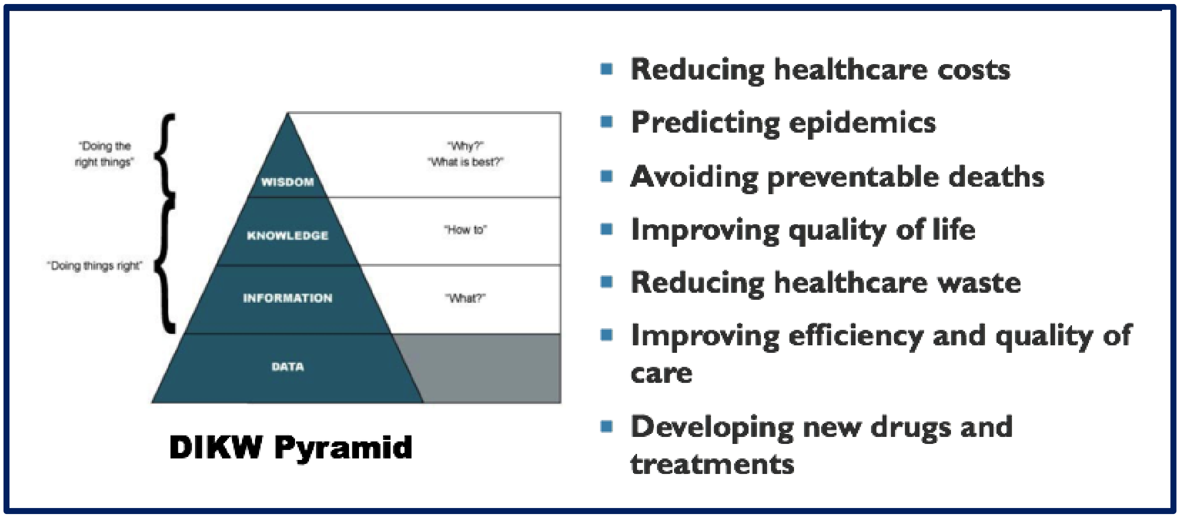

Las Vegas Ortho Clinic
Sample Data Exchange Between the Patient and Organizations
Rush University ER
Nevada Spine Clinic 7140 Smoke Ranch Rd ...
Rush University Medical Group ...
DU Athletic Department
Seth is a student athlete
Las Vegas Quick Care

Figure 1. An Example of Data Exchange Between A Patient, His School and Health Providers

Patient data entered into a database are stored in repositories called data warehouses. Data warehouses centralizes and consolidates large amounts of data from multiple sources (HealtIhIt.gov, 2019). Data is then analyzed to allow researchers, universities and organizations to derive valuable business and clinical insights to improve care related decision-making processes. Over time, information builds historical records that can be invaluable to data scientists and business analysts in creating practice guidelines and standards of practice.

Data warehouses are considered an organization’s “single source of truth,” and usually include the following components: A relational database to store and manage data; An extraction, loading, and transformation (ELT) solution for preparing the data for analysis; Statistical analysis, reporting, and data mining capabilities; Client analysis tools for visualizing and presenting data to users; Analytical applications that generate actionable information. In healthcare, data warehouses produce knowledge that is used as basis for decision making in healthcare. Figure 2 below shows how data is processed to drive decisions that impact healthcare.



- Reducing healthcare costs
- Predicting epidemics
- Avoiding preventable deaths
- Improving quality of life
- Reducing healthcare waste
- Improving efficiency and quality of care
- Developing new drugs and treatments

Figure 2. Data, Information, Knowledge, Wisdom Pyramid and How it Impacts Healthcare

With the automation of patient's records, healthcare is now one of the biggest industries that utilizes technology as a support infrastructure. Today, 30% of the world's data is coming from the healthcare industry. The digitalization and automation of data entry comes from various platforms including personal patient entry, telemedicine, telepsychiatry and use of mobile healthcare technology platforms. Health information technology, through data science and predictive analytics can reduce healthcare cost, predict epidemics, avoid preventable deaths, reduce healthcare waste, ensure safety and quality of care and improve people's overall quality of life. Research to document and evaluate outcomes of care also serve as basis for supporting new drug and treatment regimen. To achieve these goals, data from various points of entry, various sources need to be entered, stored, managed, secured, transferred, shared, analyzed, converted into knowledge, and finally, reported. Figure 4 shows an example of how a third-party organization Prometheus, a company claiming to be an expert in "applying advanced informatics techniques discover and manage new knowledge from data sources relating to health, repurpose that knowledge and use it to improve care and outcomes."

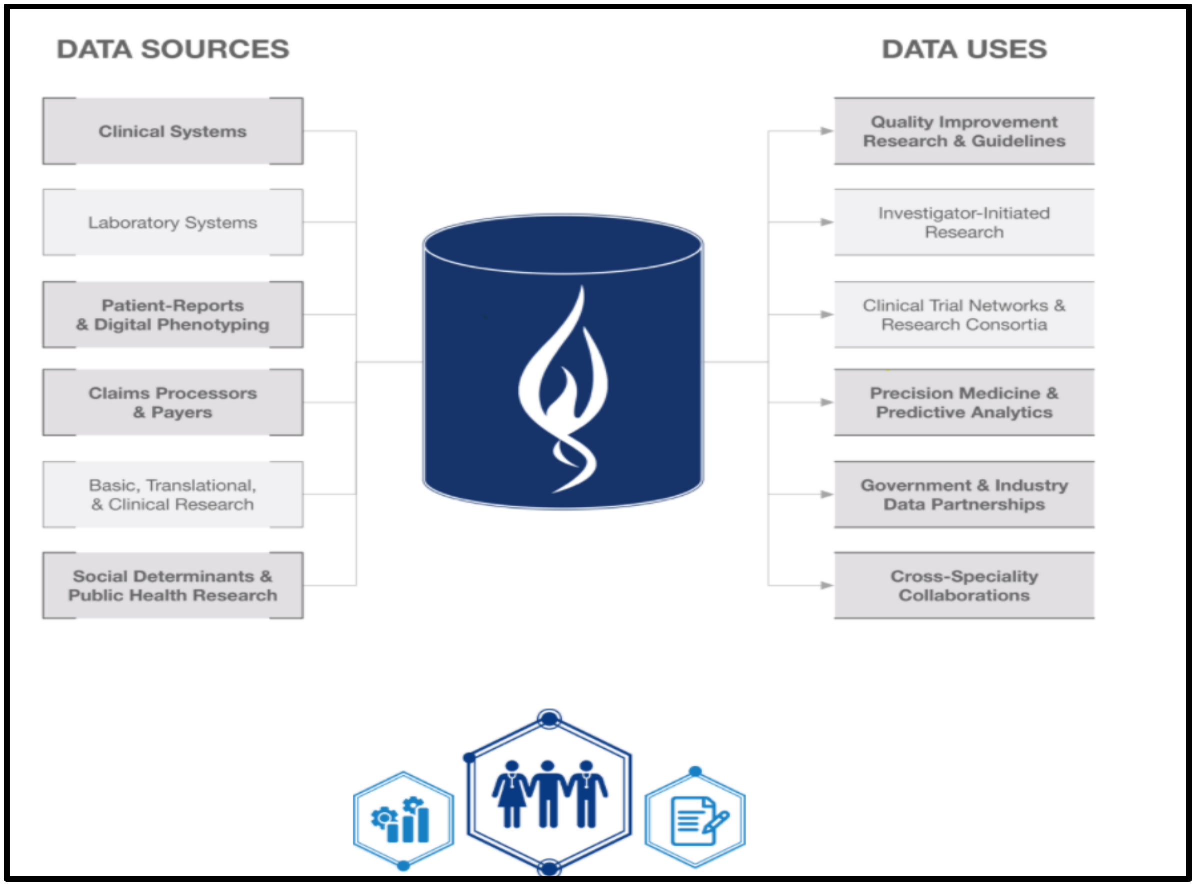

DATA SOURCES
Clinical Systems
Laboratory Systems
Patient-Reports & Digital Phenotyping
Claims Processors & Payers
Basic, Translational, & Clinical Research
Social Determinants & Public Health Research
DATA USES
Quality Improvement Research & Guidelines
Investigator-Initiated Research
Clinical Trial Networks & Research Consortia
Precision Medicine & Predictive Analytics
Government & Industry Data Partnerships
Cross-Speciality Collaborations

Figure 3. The company Prometheus research promotes "RexRegistry," which is a platform that offers its subscribers high quality data that can be used for different initiatives, including education, advocacy, and research. https://www.prometheusresearch.com/

LITERATURE REVIEW

Security Threats in Healthcare

According to the Federal Bureau of Investigation, computer or cybercrimes are defined as acts performed by hackers that illegally access, manipulate or acquire another's or a company's data and use, destroy, corrupt information to the detriment of its owner. As the growth of storing data is expanding rapidly, so does its vulnerability to cyberattacks. In an article written by Kevin Murray (2019), he states that the healthcare industry is one of the most sought-after targets for cybercriminals because medical data is worth 10 times more than information from a person's credit card. He also states that a single hospital has several departments that store patient information, "a one stop shop" for data criminals. The liability in health information technology extends far beyond patient demographics, data management, analytics, cloud and storage (Murray, 2019). The same author continues to say that clinical drug trials, information from medical devices that are being tested, consumer use of mobile technology and apps as well as state and government funded initiatives that cost millions of dollars could be lost in one breach. FBI records show that healthcare attacks are done using malware, including trojans that steal employee credentials and infiltrate networks; Insider threats; Supply chain compromise, including breaches at third-party companies that store patient records; Lost devices, including smartphones and laptops; Poor patching procedures for software used by medical organizations; Lack of staff training, and human error as well as outdated systems. According to IBM's 2019 annual study on Cost of Data Breaches revealed that an average data breach can cost up to $3.9 million. For the ninth year in a row healthcare organization incur the highest cost which was close to $6.5 million.

Phoenixnap.com in July 2019, published a summary of a survey on healthcare organizations and their experiences on data breaches:

- 89% of healthcare organizations experienced a data breach in the past two years. Despite the sophisticated measures put in place by providers to prevent data breaches, they are still common.
- A Mid-Horizon study concluded that approximately 100 percent of web applications connected to critical health information is vulnerable to cyberattacks. Network penetration results also showed that hackers could easily access domain level admin privileges of most healthcare applications. As a result, the use of advanced technologies such as block-chain and cloud computing are necessary to ward off such attacks in the future.
- It is estimated that the loss of data and related failures will cost healthcare companies nearly $6 trillion in damages in the next three years compared to $3 trillion, in 2017.

From a statistical point of view, it is the most significant transfer of wealth in human history. If proper security measures are not taken, experts believe that cybercrime can have a devastating financial impact on the healthcare sector in the next four to five years.

- 82% of surveyed healthcare organizations agree that digital security is one of their foremost concerns.
- 55% of healthcare companies in the United States faced cyberattacks. Almost one-fifth confirmed that they had been attacked in the last 12 months.

Sample Data Breaches in Healthcare

Ransomware, according to the Phoenixnap.com (a large international datacenter), continues to be one of the biggest threats in healthcare for 2019, and beyond 2020. There has been a documented 80% increase in the number of people that fall victim to data breach from 2017 to 2020 (Phoenixnap.com, 2020). The healthcare sector is prone to paying the ransom because the disruption, lost productivity, and damage to the data can be more expansive than preventing the loss by paying the ransom. Healthcare organizations are more willing to pay ransom to avoid downtime and gain access to critical patient data. It is estimated that 23 percent of healthcare organizations paid some form of payment to the attackers. Techrepublic.com reports that medical records could go between $250.00 to $500.00 (black market ransom) a record depending on what information the medical record contains. The majority of healthcare ransomware attacks were malware related. Of the 2,600 incidents reported, 36 percent were malware related followed by accidental disclosure in 26 percent of the cases. The healthcare industry has lost over 2 trillion dollars from cybercrimes in 2019 (Sobers, 2020).

DATA BREACH PROCESS MODEL AND SAMPLE SECURITY INCIDENTS

Trend Micro (2018) summarized the process on how data breach occurs. First the cybercriminal does research and tries to find weakness in the organization’s system, then an attack is initiate through a network or a social attack using an infrastructure, system, or an application to infiltrate the organization's network. An example is sending an email to employees prompting them to log on to a site using their credentials or sending emails to employees asking them to open an email containing a malicious attachment. Once the criminal is able to steal an employee's log on information, they will assume that employee's identity and remotely log on into one computer. If undetected, the criminal will be able to work his/her way into accessing all the files within the organization. (Refer to Figure 4).

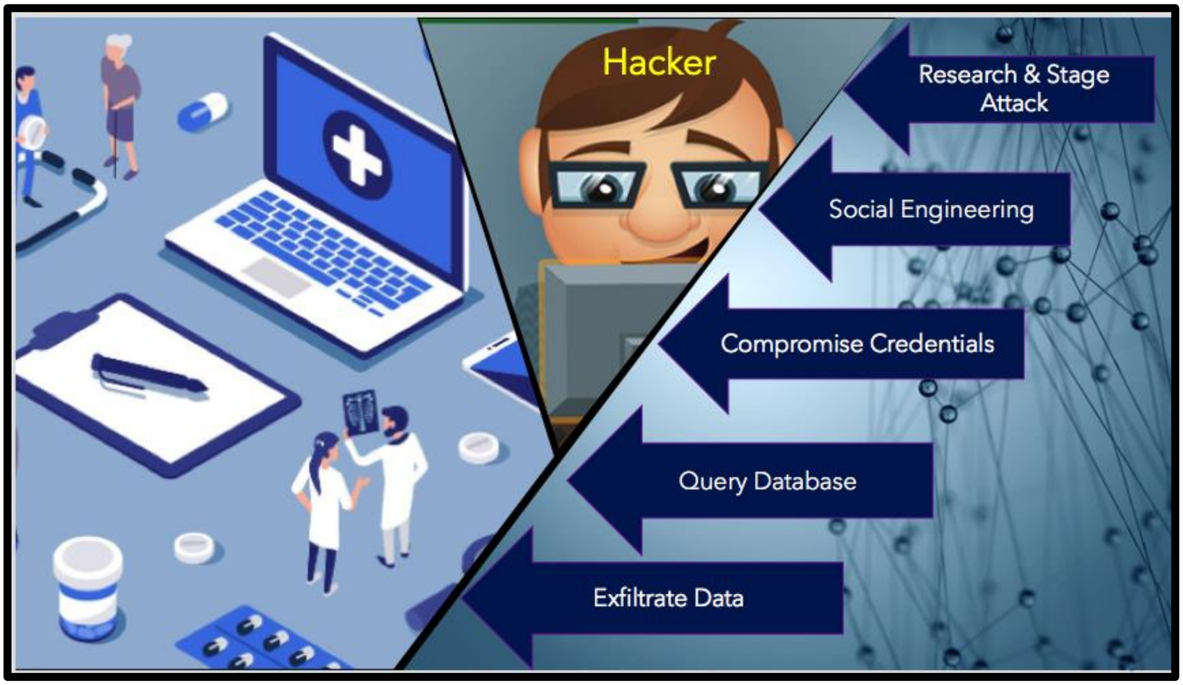


Figure 4 Stages of a Data Breach Diagram: Hackers Troll and Look for Weakness in the System

Anthem Data Breach

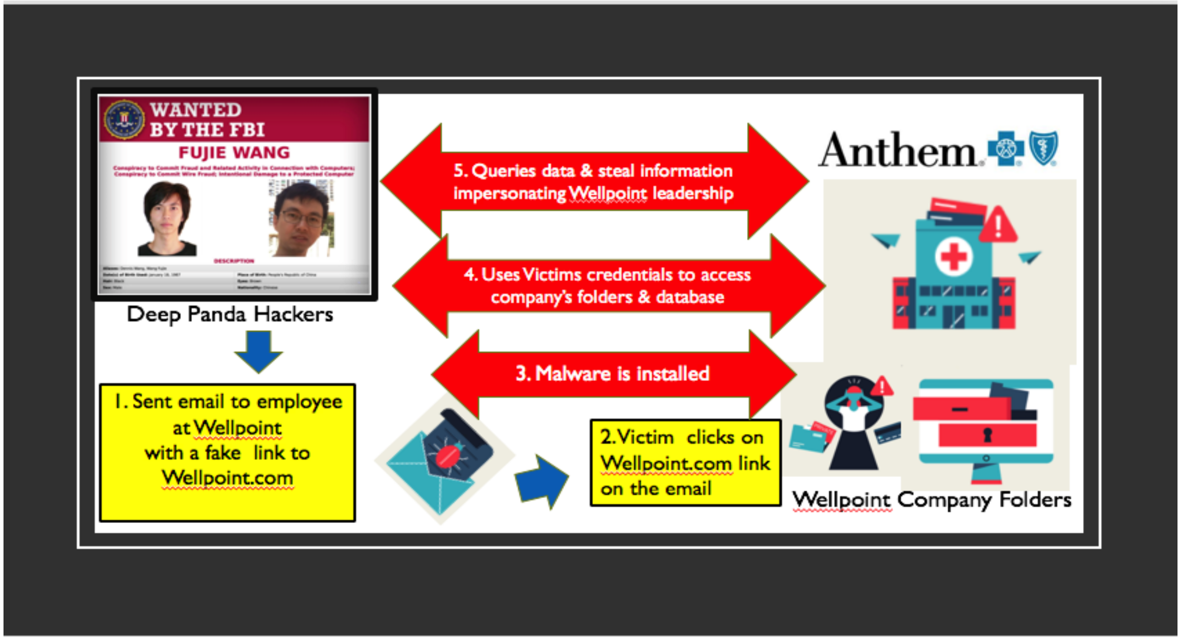
U.S. health insurance giant Anthem Blue Cross Blue Shield stated that in April, 2014, it had suffered a massive data breach, which led to the compromise of more than 80 million customer records (Tabaa, 2019). Anthem continued to report that the company hired security experts and discovered that the attack that was collectively known as Deep Panda. The attack was launched from China through the Scanbox Framework. The framework was composed of a suite of tools that have been used in a number of cyber espionage attacks but caught the insurance company unprepared. According Sienko (2019) in an article he wrote for Information Security

Institute, Anthem failed to encrypt the huge volume of personal information it held, however, HIPAA doesn’t require insurance companies to encrypt its data.

The hackers were able to get network credentials for multiple individuals within the company who had high-level access to the IT system through some phishing attacks and installed malware on devices of people in company leadership (Tabaa, 2019). The malicious emails launched the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and dozens of other systems within the Anthem enterprise, including Anthem's data warehouse. In December 2014, Anthem employees noticed suspicious database queries being made and this continued until the end of January 2015 (Refer to Figure 5 below). Data stolen included: Full names; Physical addresses; Email addresses; Social Security numbers; Birthdates; Insurance membership numbers; Medical IDs; Employment information and Income data.

Phishing (messages usually direct to a spoofed website or otherwise get you to divulge private information such as e.g., passphrase, credit card, or other account updates) actually triggered further scams for the company’s customers. Anthem quickly issued a warning to all members shortly after their announcement of the breach itself, warning customers about “scams designed to capture personal information, that appear as if they are from Anthem, and the emails include a ‘click here’ link for credit monitoring.” Phishing phone calls related to the breach have also been reported Tabaa, (2019) reports. Anthem urged members not to click on any links in emails, and noted that they were not calling any members. Instead, they would be limiting all correspondence to written form. The most common thing for hackers in healthcare is to sell information on the black market. Once in the hands of buyers, the information is used for identity theft, allowing nefarious individuals to take out credit cards, health insurance in a member’s name, obtain loans, and of course sell it back to the person for a fee.

How Did Phishing Scams Happen at Anthem?


WANTED
BY THE FBI
FUJIE WANG
Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer
DESCRIPTION
Anthem

Deep Panda Hackers

1. Sent email to employee at Wellpoint with a fake link to Wellpoint.com

2.Victim clicks on Wellpoint.com link on the email

3. Malware is installed

4. Uses Victims credentials to access company's folders & database

5. Queries data & steal information impersonating Wellpoint leadership

Wellpoint Company Folders

Figure 5. Hackers were able to install malware to over 50 emails before it was discovered by Wellpoint (Anthem used to be called Wellpoint) Source: https://medium.com/dataseries/take-out-how-anthem-was-breached-276b9ffca8da

In late 2015 two men from China were indicted for the crime and Anthem the company came under fire for refusing to undergo vulnerability scans and configuration compliance tests in 2015. As part of a litigation settlement, Anthem said it would pay $115 million – the funds would mostly go towards two years of credit monitoring for the breach's victims. And in 2018, Anthem agreed to pay $16 million to the U.S. government for HIPAA violations.

Other Healthcare Cybercrimes according to Phoenixnap.com include the following: (Source: https://phoenixnap.com/blog/healthcare-cybersecurity-statistics)

LifeBridge Health. This Baltimore-based healthcare system experienced a malware attack last March. The attack potentially breached the data of around 500,000 patients. Investigations showed that the hackers first gained access to the system back in September 2016.

Health Management Concepts. This ransomware attack fast became a full-blown data breach. Hackers were mistakenly provided with a file containing the personal data of over 500,000 patients. The organization has not disclosed how or why hackers got this information, but the file contained Social Security numbers, health insurance information, and patient names.

CNO Financial Group. Between May and September of last year, hackers gained access to the credentials of CNO employees. This information was then used to access company websites, compromising the data of over 566,000 policyholders and applicants. Data accessed included dates of birth, insurance details, and partial Social Security numbers.

What are the cybersecurity challenges in healthcare brought about by COVID19? According to M. Hackett, Associate Editor of healthcarefinance.com, and the FBI as of March, 2020 cybercrimes in healthcare reported an increase of 400%.

- More people are logging on to their PCs working from home (remotely)
- People are using their computers and credit cards to shop, donate, order, etc.
- Students are using their PCs to access their classes through online platforms
- Increased use of devices: phones, IPADs etc.
- Increased use of social media/and meeting platforms that may not have the capability to provide security and privacy to a sudden surge in users
- Inexperienced users open phishing scams & fall victim to malwares, & hackers

It is important for both the private sector be to aware that cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware. Human factors such as curiosity, concern, boredom, need to socialize, obtain information or even access money or rewards are being used to tempt the public to click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware. For example, e, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install "CovidLock" ransomware on their device. In some cases, malware would contain email subject lines such as “Coronavirus Update” or “2019-nCov: Coronavirus outbreak in your city (Emergency).” World Health Organization (WHO) or an individual with “Dr.” in their title. In several examples, actors send phishing emails that contain links to a fake email login page. Other emails purport to be from an organization’s human resources (HR) department and advise the employee to open the attachment.

Healthcare organizations should warn their employees and consumers against opening emails that contain “COVID19 Test results” that ask for personal information, etc. Healthcare related organizations in order to safeguard its consumers against cybercrimes, should re-evaluate current security policies and procedures and adopt new ones based on need.

SECURITY POLICY

HHS through HealthIT.gov offer templates for IT security policies based on organizational requirements such as confidentiality, integrity, and availability. HIT.gov recommends that in developing policies, the organization’s entire data network, whole range of data assets, from the data’s point of origin and through all points of transit, storage, security gaps, results of assessment of access controls (encryption, authentication, authorization), existing procedures to address breach, relevant potential hazards, including special risk circumstances and industry-specific compliance regulations should be considered. Leaders should also look at adopting policies that address penalties for violations, such as revocation of credentials and denial of access, etc. A periodic review of the company’s policies and procedures is necessary to keep up with current trends to make sure that new threats are met. Whenever the company expands its operations, a review should be done, both to make sure the current program is up-to-date and to account for any new issue that the expansion may introduce.

The consequences of cybercrimes come at a high price for healthcare organizations, its customers, and its investors. Most healthcare organizations hire Chief Informatics Officers who lead teams from different departments including risk management to develop health information technology policies and procedures. Cybersecurity has also become such a huge business that there are a multitude of companies competing to offer comprehensive cyber security services that range from simple spyware, to comprehensive systemwide security systems and templates for policies and procedures that organizations can adapt and customize to satisfy audit requirements, adhere to best practices, mitigate risk from a security incident, educated users on sound security practices, reduce legal risk, assure stakeholders and consumers and meet compliance with: The PCI Data Security Standard (DSS) 3.0, HIPAA, The Sarbanes-Oxley Act (SOX), FDA Title 21 CFR Part 11, SAS 70, ISO 17799Existing resources, such as those available through HIT.Gov, the Agency for Healthcare Research and Quality (AHRQ), and the Electronic Healthcare Network Accreditation Commission (EHNAC) accreditation guidelines, provide healthcare organizations and individual healthcare providers guidance on health information exchange. According to Cisco, a large HIT company states that police should comply with Confidentiality (sensitive information are accessed only by an authorized person through the use of security mechanisms such as usernames, passwords, access control lists (ACLs), and encryption.) Integrity (data is true and correct to its original purposes; can be done through data encryption and hashing). Finally, data should be available (information and resources are available to those who need them, through hardware maintenance, software patching and network optimization).

Connecting for Health Common Framework provides a policy matrix that includes strategies for developing HIE policies and procedures. Sample contents of healthcare information policies and procedures should include but not limited to: Acceptable Use Policy, Password Policy, Backup Policy, Network Access Policy, Incident Response Policy, Remote Access Policy, Email Policy, Guest Access Policy, Wireless Policy, Third Party Connection Policy, Network Security Policy, Encryption Policy, Confidential Data Policy, Data Classification Policy, Mobile Device Policy, Retention Policy, Outsourcing Policy, Physical Security Policy, Virtual Private Network (VPN) Policy. In addition to the policies, Policy Acknowledgement Forms, Security Incident Report, Notice of Policy Noncompliance, Account Setup Request, Guest Access Request, Request for Policy Exemption and Education Acknowledgement Form is also included in the policy handbook. All end users and employees should be educated on the organization’s HIT policies.

RECOMMENDATIONS

Leffel (2017), the VP of Network and Cloud Security of Digital Guardian, stated that the goal of healthcare industries is to deliver quality patient care using technology. This also means complying with the strict regulatory requirements set forth by HIPAA and other regulations, such as the EU's General Data Protection Regulation (GDPR). Because protected health information (PHI) is among an individual's most sensitive (and for criminals, valuable) private data, the guidelines for healthcare providers and other organizations that handle, use, or transmit patient information include strict data protection requirements that can require fines if they're not met (Leffel, 2017). The following security tips are for both healthcare organizations and its staff:

Educating Healthcare Staff

It is recommended that healthcare staff should attend classes that help them understand HIPAA and PHI rules and regulations as well as policies and procedures. Security awareness training equips healthcare employees with the requisite knowledge necessary for making smart decisions and using appropriate caution when handling patient data. End users should also be educated on the following:

- Errors in grammar: Phishing emails often contain spelling or grammar mistakes, or are sent from dodgy-looking addresses that resemble the company being impersonated. Look carefully for any warning signs that might indicate that the email is a fraud.
- Free giveaways and gifts: There's no such thing as a 'free gift'! If emails contain special offers, free memberships, discounted products etc., it is likely a scam. It is advised to manually enter the website of the company you're looking to buy from, and not click on links sent to you. Also, never provide information before double, and triple checking the authenticity.
- Use strong passwords: Avoid falling into the 'obvious password traps' by using things like name or date of birth or any other personal information. Ensure unique

passwords for each different service. Numbers can be used to replace letters, to make the password stronger e.g. MyTe@msL0g1n

- Updates: Make sure, when prompted, emphasize installing app security updates.

Recommendations for healthcare organizations

Restricting Access to Data and Applications Access restrictions require user authentication, ensuring that only authorized users have access to protected data. Multi-factor authentication, which requires users to validate their identity through two or more validation methods, is a highly-recommended approach.

Implementing Data Usage Controls

Protective data controls go beyond the benefits of access controls and monitoring to ensure that risky or malicious data activity can be flagged and/or blocked in real time. Healthcare organizations can use data controls to block specific actions involving sensitive data, such as web uploads, unauthorized email sends, copying to external drives, or printing. Data discovery and classification play an important supporting role in this process by ensuring that sensitive data can be identified and tagged to receive the proper level of protection.

Logging and Monitoring Use

Logging all access and usage data is also crucial, enabling providers and business partners to monitor which users are accessing what information, applications, and other resources, when they are being accessed, and from what devices and locations. These logs prove value for auditing purposes, by identifying areas of concern and strengthening protective measures when necessary. When an incident occurs, an audit trail may enable organizations to pinpoint precise entry points, determine the cause, and evaluate damages.

Encrypting Data

Encryption is one of the most useful data protection methods for healthcare organizations. By encrypting data in transit and at rest, healthcare providers and business partners make it more difficult (ideally impossible) for attackers to decipher patient information even if they gain access to the data.

Securing Mobile Devices

Increasingly, healthcare providers and covered entities utilize mobile devices to access information to help treat a patient, or to process insurance claims.

Mitigating Connected Device Risks

In healthcare, medical devices like blood pressure monitors and cameras for monitoring physical security on the premises may be connected to a network.

Some tips for maintaining adequate connected device security include:

Conducting Regular Risk Assessments

By evaluating risk across the organization periodically to proactively identify and mitigate potential risks, healthcare providers and their partners can more effectively prevent costly data breaches and avoid the many other detrimental impacts of a breach, from reputation damage to penalties issued by regulatory agencies.

Utilizing Off-Site Data Backup

As many ransomware attacks have shown, cyberattacks can expose sensitive patient information but they can also compromise data integrity or availability. Natural disasters can have major consequences on data centers if data isn’t properly backed up.

Carefully Evaluating the Compliance of Business Associates

Because healthcare information is increasingly transmitted between providers and among covered entities to help facilitate payments and deliver care, a thorough evaluation of all potential business partners is one of the most crucial security measures healthcare organizations can take.

Just as healthcare is a partnership between providers and consumers, cybersecurity in healthcare require consumers to be just as knowledgeable and accountable as the healthcare organizations that provide services. Consumers need to be aware about cybercrimes and how personal information, and sensitive data such as medical records can potentially be sold at the black market, or can be used to obtain medical insurance for and by another individual.

CONCLUSION

Health Information Technology according to healthcare.gov is defined as the electronic systems health care professionals – and increasingly, patients – use to store, share, and analyze health information. It includes electronic health records (EHR) where doctors keep track of consumer's health records and share it with other providers; personal health records or PHR where patients can enter their information based on medical EHR plus personal preferences; E-prescribing where doctors can enter prescription for medications. All of these tools were meant to assist in keeping people healthy in an efficient, cost effective, timely, safe and secure manner through information sharing. However, as technology progresses, cybercriminal prey on human flaws as well as the weaknesses of automated systems. In today's world, where risk is inevitable, the call for cybersecurity experts to work with healthcare process flow experts is crucial in anticipating and preventing healthcare cybercrimes to occur. The responsibilities lie in organizations in making the security, safety and privacy of their consumers a priority. The Federal government has to remain vigilant in creating mechanisms of checks and balance in the form of policies and regulation standards and laws to punish cybercriminals and unethical IT business practices. Consumers, should be active participants in protecting their health-related data and work in collaboration with organizations in establishing policies that would protect the public from threats to privacy and security. With COVID19, the new normal in healthcare is evolving. Technology will continue to be an important tool for the public in any aspect of life specially in healthcare, but it will come with a price. The question is: are we all willing to pay the price?

REFERENCES

Cybersecurity in healthcare threats and impact. Accessed from https://www.gehealthcare.com/infographics/infographic-cybersecurity-in-healthcare---threats-and-impact

Dobran, B. (2019). 31 Must know cybersecurity statistics. Accessed from https://phoenixnap.com/blog/healthcare-cybersecurity-statistics

Fraudwatch. COVID19 has long term effects on cybersecurity. Accessed from https://fraudwatchinternational.com/active-scams/covid-19-has-long-term-effects-on-cyber-security/

Hackett, M., (2020). Healthcare Finance. "Number of cybersecurity attacks increases during COVID-19 crisis: Hackers are taking advantage of provider distraction to breach health systems." Accessed from https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis

Health IT. Laws, Regulation and Policy. Accessed from https://www.healthit.gov/topic/laws-regulation-and-policy

Health IT. Privacy, Security and HIPAA. Accessed from https://www.healthit.gov/topic/privacy-security-and-hipaa

Healthcare cybersecurity. Accessed from https://www.fortinet.com/solutions/industries/healthcare.html?utm_source=blog&utm_campaign=2018-q2-healthcare-page

How Big Data Analytics drives Healthcare Industry? Accessed from https://www.loginworks.com/blogs/data-analytics/how-big-data-analytics-drives-healthcare-industry/

IBM Data Breach Calculator. Accessed from https://databreachcalculator.mybluemix.net/

Kumari, A., Tanwar, S., Tyagi S., and Kumar, N. (2019). "Verification and validation techniques for streaming big data analytics in internet of things environment," in IET Networks, vol. 8, no. 3, pp. 155-163, 5 2019, doi: 10.1049/iet-net.2018.5187.

Leffel, C. Healthcare Cybersecurity: 10 Tips for Keeping Private Health Data Secure. Accessed from https://hitconsultant.net/2017/07/25/tips-private-health-data-secure/#.Xo-EstOpGCU

Murray, K. (2019). Accessed from https://www.webroot.com/blog/2019/10/24/why-healthcare-organizations-are-easy-targets-for-cybercrime/

Sobers, R. (2020). Data Security: 107 Must-Know Data Breach Statistics for 2020. Accessed from https://www.varonis.com/blog/data-breach-statistics/

Sienko, C. Infosec. The Breach of Anthem Health. Accessed from https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/case-study-health-insurer-anthem/#gref

Tabaa, B. (2019). Dataseries: Takeout-How Anthem was breached. Accessed from https://medium.com/dataseries/take-out-how-anthem-was-breached-276b9ffca8da

Trend Micro (2018). Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes. Accessed from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

The impact of technology in healthcare. Accessed from https://www.aimseducation.edu/blog/the-impact-of-technology-on-healthcare/