Table of Contents

An Insight into the Current Security Posture of Healthcare IT: A National Security Concern

Authored by: Jessica Brewer, Vasavi Hejjaji, Leo Ip, Brandon Ta, and Zhuoxue Wu

Introduction

Over the past decade, technology has worked to augment the healthcare industry. Leveraging the advancements of medical devices and the improvements in communication technology, healthcare providers now have access to faster, more accurate data to improve patient care. While the use of this technology has aided providers in offering better services to their patients, it also comes with the price of an ever-expanding threat landscape. The increased use of connected medical devices has made healthcare facilities more vulnerable to cyber attacks. Medical devices worn by patients have become caches of valuable information targeted by hackers. The supply chain that was established to support healthcare technology has become a complex, global process, exposing healthcare facilities and device manufacturers to premeditated external risks. Employees with access to sensitive data can compromise it with the click of a button. Most notably, though, is the peculiarity of the healthcare industry as it relates to cybersecurity. In most industries, cyber attacks affect workflow and these disruptions often influence revenue and reputation. In healthcare, however, a cyber attack can mean the difference between life and death.

The healthcare industry faces a unique dilemma: how do they balance their cybersecurity needs while still providing fast and efficient patient care? In this paper we seek to answer that question by enumerating the cyber threat landscape of the healthcare industry as it relates to US national security. We analyze the traditional threats posed by ransomware and insiders, to the future threats generated by connected devices, supply chain vulnerabilities, and emerging technologies. In addition to detailing these threats, we discuss the role of technology as a mitigating solution. Specifically, we propose how healthcare organizations can leverage artificial intelligence, machine learning, and blockchain along with relevant frameworks, policies, and procedures to greatly reduce these risks.

Threats Affecting the Healthcare Industry

With the healthcare industry development, more threats based on new technology have emerged. This section introduces the external threats to data and privacy in healthcare information systems and healthcare disruption caused by malware and ransomware. In addition, the internal threats also need be considered. Although it is the threat through all times, it needs more attention because of increasing the adaptation of technology in healthcare.

Healthcare Information Systems and Potential Threats

The practice of complementing traditional healthcare services with the convenience and capabilities that the internet affords has allowed for significant improvements in patient care, particularly in the diagnosis and treatment phases. To increase the adaptation of technology in healthcare, the HITECH Act has encouraged healthcare facilities to implement electronic health records.[1] However, integrating these connections also has the side effect of introducing threats that the healthcare industry has not historically experienced before. Patient health information is generally stored in a digital format, known as an Electronic Health Record (EHR). While these EHRs can improve the efficiency of the healthcare industry and patient experience writ large, the push to introduce more connected medical services and EHRs will increase the number of vulnerable healthcare organizations leading to an increase in stolen medical records. Between 2015 and 2018, the number of healthcare institutions that suffered from cyber a[2] increased from 20% to 40%.[3]

According to Black Book Market Research, over 90 percent of healthcare organizations have experienced a data breach since Q3 2016, with nearly half suffering more than 5 breaches. There are also low confidence for the future of security as only 12 percent of hospitals believes that their security assessment will show improvement in 2019.[4] With around 3 percent of annual IT budgets set aside for security[5], the healthcare industry is unprepared to handle existing security threats.

Threats to Healthcare Data and Privacy

Data Breaches

A modern healthcare information system contains multiple subsystems to improve and manage patient treatments while reducing operational overhead. Within this system, confidential information such as medical histories are stored and transmitted. This data is valuable on the dark web, with some estimates placing the value of medical records at a 5 to 1 ratio compared to

---

[1] Office for Civil Rights. (2017, June 16). HITECH act enforcement interim final rule. *US Department of Health and Human Services*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

[3] Forward-Looking Threat Research (FTR) Team. (2017). Cybercrime and Other Threats Faced by the Healthcare Industry. Retrieved April 9, 2019, from https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-other-threats-faced-by-the-healthcare-industry.pdf

[4] Newswire. (2018, May 14). Black Book's Annual Cybersecurity Survey Reveals Healthcare Enterprises Are Not Maturing Fast Enough, Processes Continue Underfunded and Understaffed. Retrieved from https://www.newswire.com/news/black-books-annual-cybersecurity-survey-reveals-healthcare-enterprises-20476554

[5] Donovan, F. (2018, May 14). Healthcare Data Security Programs Get Short Shrift in IT Budgets. Retrieved from https://healthitsecurity.com/news/healthcare-data-security-programs-get-short-shrift-in-it-budgets

credit card information. Depending on the forum and quality of data, credit card information can be worth as little as $5 each, while medical information can be worth as much as $50 per record.[6] This gives malicious actors a strong financial motive to devote time and resources to breaching the systems. A successful attack can result in consequences for the hospital that can range from significant monetary loss due to regulatory fines to potential loss of human life.

On a macroscopic level, it may appear that data from different industries are equivalent in scope; however, healthcare data contains one's personally identifiable information (e.g., name, address, date of birth, etc.), medical diagnoses/history, and prescription drug information. Using this information, adversaries have the potential to impersonate victims to obtain restricted prescription medications or free medical care. This is not only damaging to victims from a monetary point of view, as they may be forced to pay for someone else's medical procedures, but it can also affect the integrity of their medical information. If an imposter updates a victim's records with erroneous medical conditions or allergies, it could pose dangers to the victim's health and affect their ability to get life insurance or a certain job. While medical ID fraud may appear difficult to perpetrate successfully, in 2013 close to two million Americans fell victim to the this growing threat.[7] Medical ID fraud is particularly damaging due to the static nature of healthcare information, which allows stolen data to remain relevant for long periods of time.[8] One can replace a credit card, but how does one replace their medical history?

The medical industry is less resistant to cyber attacks due to a reliance on legacy software and a lack of resources dedicated to security.[9] This problematic situation, along with the value of their data makes the industry a ripe target for attackers. From January to October 2015, data breaches of healthcare organizations have affected over 110 million US citizens. The average cost for victims to recover from medical identity theft is $13,500. The increased reliance of the industry on electronic communications will only serve to further escalate the security issue. The Ponemon Institute estimates that these cyber attacks cost the industry $6 billion annually.[10] With such a high cost, it would be advisable to increase investments in security to mitigate future loses.

---

[6] Richard. (2017, July 01). The value of stolen data on the dark web. Retrieved from https://darkwebnews.com/dark-web/value-of-stolen-data-dark-web/

[7] Gardner, E. (2014, August 18). When the patient is an imposter. *US News and World Report*. Retrieved from https://health.usnews.com/health-news/patient-advice/articles/2014/08/18/when-the-patient-is-an-impostor

[8] Humer, C. & Finkle, J. (2014, September 24). Your medical record is worth more to hackers than your credit card. *Reuters*. Retrieved from https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

[9] Wetsman, N. (2019, April 04). Health care's huge cybersecurity problem. Retrieved from https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

[10] Socas, J. (2015, December 21). Growing pains: cybercrime plagues the healthcare industry. *Healthcare IT News*. Retrieved from https://www.healthcareitnews.com/blog/growing-pains-cybercrime-plagues-healthcare-industry?utm_content=bufferc1733&utm_medium=social&utm_source=plus.google.com&utm_campaign=buffer

Information Disclosure

Encryption is often considered an effective mitigating solution for information disclosure threats as it prevents stolen data from being read; however, certain encryption schemes are vulnerable to attacks. In exchange for improved security, encrypted data requires additional processing time to access; without timely access, patients may suffer serious injuries. Additionally, encryption alone cannot fully mitigate EHRs data risks. Researchers at the University of Illinois and Portland State University have found that encrypted database systems are mostly based on CryptDB[11], which uses attribute-preserving encryption schemes such as deterministic (DTE) and order-preserving encryption (OPE). This type of encryption scheme is vulnerable to frequency analysis and sequencing, and attack strategies based on combinatorial optimization. In a study to determine the efficacy of these attacks in an empirical setting, researchers were able to recover 80 percent of encrypted patient records, including sex, names, and mortality risk.[12]

Disruptions to Healthcare

Malware and Ransomware

While disruption in other industries can influence revenue and workflow, it is particularly devastating in the healthcare field. If doctors or healthcare staff are unable to access important patient data or life-saving machines, this disruption could result in serious injury or death. In the healthcare industry, disruptions can be caused by malicious actors through the use of ransomware. This type of malware encrypts sensitive data or systems to restrict normal access. If an organization falls victim to ransomware and is in dire need to regain access to data, paying the perpetrators in the hope that the files will be decrypted is the only choice. Although some healthcare systems have redundancy systems as backups, the time for reverting is costly. However, paying the ransom does not guarantee the data decryption nor does it guarantee the integrity of the files, as they could be irreversibly damaged or modified in the process.

Traditionally, ransomware is frequently introduced to a system through phishing emails, which seeks to convince normal users to download and execute malicious attachments. Once the malware is in the system, it spreads by leveraging application vulnerabilities and improperly configured security protocols. The ransomware then propagates through the network to encrypt sensitive files and data to prevent normal operations. The full impact of such malware was shown in the 2017 Wannacry ransomware attack.

---

[11] Popa, R. A., Redfield, C. M., Zeldovich, N., & Balakrishnan, H. (2011). CryptDB. *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles - SOSP 11*. doi:10.1145/2043556.2043566

[12] Naveed, M., Kamara, S. & Wright, C. (2015, October). Inference attacks on property-preserving encrypted databases. *SIGSAC Conference on Computer and Communications Security*. Retrieved from https://cs.brown.edu/~seny/pubs/edb.pdf

WannaCry first appeared in May 2017 and spread globally by exploiting machines that were not fully patched. Once installed, the virus encrypted computers and asked victims to send $300 USD worth of bitcoin to receive the decryption key.[13] WannaCry affected companies such as FedEx in the US and Telefonica in Spain, as well as the United Kingdom's National Health Service (NHS).[14] The NHS in particular was hit hard by the ransomware. According the NHS, 80 out of 236 service providers within its network were affected, leading to over 19,000 appointment cancellations. Although they did not pay the ransom, the disruption caused by WannaCry cost the NHS nearly 120 million dollars.[15]

Distributed Denial of Service Attack (DDoS)

Distributed Denial of Service (DDoS) attacks are another threat that the modern healthcare industry faces. This type of attack utilizes hundreds of compromised devices, known as a botnet, to overload the network until services become unavailable. In 2014, Boston Children's Hospital was involved in a controversial 14-year-old patient custody case. The sensitivity of the case prompted the hacker group "Anonymous" to launch a week-long DDoS attack causing nearly $300,000 in damages.[16]

Attacks that disrupt the availability of services can be coordinated with a terrorist attack. This deadly combination seeks to overwhelm hospitals while causing massive casualties. With non-functioning equipment and unavailable patient data, hospitals would be unable to provide medical services. They would be forced to transfer their patients to facilities that were not affected by the attack. The transportation of the injured will requires additional manpower and the transfer time can negatively impact their treatment and survivability. Furthermore, these unaffected facilities may be overwhelmed as they might not be equipped for the increased workload. This type of coordinated attack could have devastating consequences for the nation.

---

[13] Morse, A. (2018, April 24). Investigation: WannaCry cyber attack and the NHS. Retrieved from https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

[14] Lee, M., Mercer, W., Rascagneres, P., & Williams, C. (2017, May 12). Player 3 Has Entered the Game: Say Hello to 'WannaCry'. Retrieved from https://blog.talosintelligence.com/2017/05/wannacry.html

[15] Palmer, D. (2018, October 12). This is how much the WannaCry ransomware attack cost the NHS. Retrieved from https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/

[16] United States Attorney's Office District of Massachusetts. (2018, August 1). Jury convicts man who hacked boston children's hospital and wayside youth & family support network. *US Department of Justice*. Retrieved from https://www.justice.gov/usao-ma/pr/jury-convicts-man-who-hacked-boston-childrens-hospital-and-wayside-youth-family-support

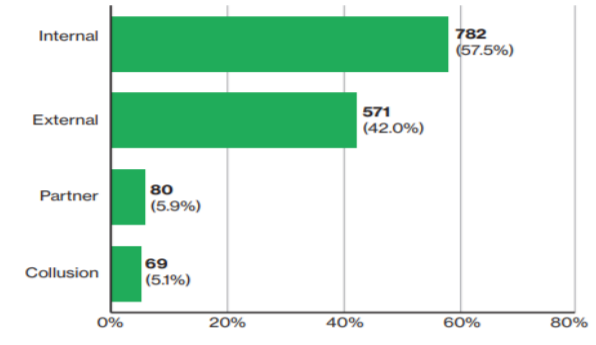
Internal Threats Affecting Healthcare Security

Bring Your Own Device (BYOD)

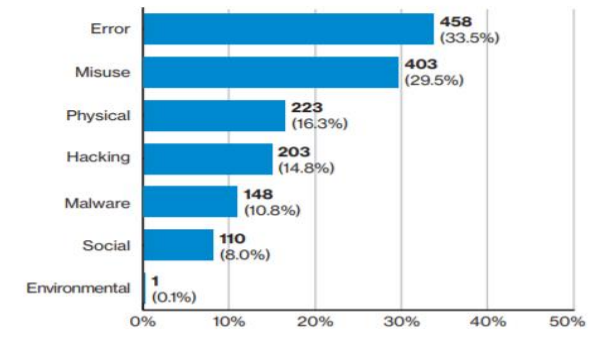
An increasing number of institutions are implementing Bring Your Own Device (BYOD) policies.[17] By allowing employees to use their personal devices for business purposes, these policies increase the organization's threat landscape. Personal devices can be infected with malware and circumvent existing security measures within the protected company network. These devices may also fail to comply with the strict security standards employer-provided devices must follow. Despite these inherent security vulnerabilities, a study by the Ponemon Institute found that 81% of healthcare providers have implemented a BYOD policy. The study further noted that few organizations had implemented adequate security measures to mitigate the threats. In total, only 59% of companies required anti-virus software to be installed and less than 50% required any form of management software.[18]

Insider Threats

The security of a healthcare facility is only as strong as its weakest link. Although sophisticated external threats may seem to pose as the biggest risks to healthcare facilities, a 2018 Verizon data breach report found that most threat actors were internal such as employees of the healthcare organization (Figure 1). Almost 60% of incidents involved insiders and, according to the report, "healthcare is the only industry in which internal actors are the biggest threat to an organization". Among these insider threat actors, the majority of them either handled data erroneously (33.5%) or misused data (29.5%) resulting in a reportable data breach (Figure 2).[19]



Threat Actors
Fig. 1 Threat Actors in Healthcare (Verizon)



Threat Actions
Fig. 2 Threat Action Categories (Verizon)

[17] Poremba, S. (2019, January 24). As BYOD Adoption Increases, Can Enterprise Data Security Keep Up? Retrieved from https://securityintelligence.com/as-byod-adoption-and-mobile-threats-increase-can-enterprise-data-security-keep-up/

[18] Ponemon Institute. (2014, March). The Cost of Insecure Mobile Devices in the Workplace. Retrieved from https://www.ponemon.org/local/upload/file/AT%26T%20Mobility%20Report%20FINAL%202.pdf

[19] Verizon. (2018). Protected health information data breach report. *Verizon Enterprise*. Retrieved from http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

While some insider threats are perpetrated by disgruntled employees or those with criminal motivations, not all insider threats are malicious. Some insider threats are constituted as negligent or accidental insiders. These insiders abuse the insufficient access controls on medical records, which are often reduced in an effort to improve the efficiency of healthcare services offered by providers.[20] For example, two employees improperly accessed personal health information from 115,000 patients, Memorial Healthcare Systems paid a $5.5 million fine for HIPAA violations which otherwise could be used for patient care.[21] Although patient care is paramount, stricter access controls can help mitigate insider threats with minimal impact to quality of care.

Security Threats for Connected Devices in the Healthcare Industry

Improvements to the flow of information have enabled businesses to become more effective and efficient. In the past, hospitals have utilized unconnected technology to provide patient care, but with the improvement of communication technology, hospitals are now leveraging connectivity to improve their quality of care. Devices which feature internet connectivity and remote communications are known as the Internet of Things (IoT). While IoT devices can provide many benefits, they can also increase information security risks and potentially harm patients. These vulnerabilities can not only have devastating effects on individual patients but can also be tailored to target specific government organizations to cause national security incidents.

The Expanding Attack Surface

The use of IoT increases the attack surface and exposure to cyber threats for healthcare providers. Imagine building fences around a farm, with a larger landmass, a longer fence would be required. At the same time, as the fencing expands, more resources must be used to manage the perimeter. Incorporating IoT devices into an environment is similar; the more devices you connect to a network, the greater security exposure you create.

The attack surface illustrates the challenges of protecting information. When connected to a network, computed tomography (CT) scan results can be more exposed. Although networked CT scans offer many benefits, they can hypothetically allow a 3rd party to remotely extract the results. This provides an additional avenue for unauthorized access to sensitive data.

---

[20] Byers, C. (2018, February 13). These data security challenges are plaguing the healthcare industry. Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/these-data-security-challenges-are-plaguing-the-healthcare-industry.html

[21] Byers, J. (2017, February 16). Memorial Healthcare Systems to pay $5.5M over potential HIPAA violations. *Healthcare Dive*. Retrieved from https://www.healthcaredive.com/news/memorial-healthcare-systems-to-pay-55m-over-potential-hipaa-violations/436400/

Compatibility with the Internet of Things

An electronic health record (EHR) system can improve the quality of healthcare by providing a centralized location for healthcare practitioners to access patient information. However, many existing EHR systems are not compatible with IoT devices, and this interoperability may prevent the data gathered from the IoT devices from being communicated to a central location. Although some EHR systems can be used to manually import the data[22], further developments may be required to automate the import process and effectively integrate IoT devices into EHR systems.

While improvements to EHR systems and IoT compatibility can improve the efficiency of operations, it can also introduce new threats. For example, additional software and hardware can be used to temporarily store data gathered by IoT devices and modify it into an EHR-compatible file format. In this example, the attack surface increases through the introduction of the hardware to store the data and the software used to manipulate it. If either of these failed, by malicious means or otherwise, the whole system could fail. Furthermore, having the data flow through three nodes instead of two creates an additional entry point for unauthorized access, further highlighting the difficulty in managing connected devices.

Connected Devices and Confidentiality

When considering security incidents, it is important to consider both the possibility of both malicious attacks and negligence. IoT devices store, collect, and process patient data, which increases the possibility of confidentiality concerns. Many of these devices enable remote patient monitoring and alerts. For example, activity tracking devices such as Fitbits store more than 150 billion hours of heart rate data.[23] While Fitbits are not used as medical devices, researchers at the Charotar University of Science and Technology had prototyped a similar device to detect heart attacks using patient heart rate. In their experiment, an alert is automatically sent to an external device when a heart attack is detected.[24] This has useful real-world implications as these alerts can be sent to doctors or hospitals if anomalous behavior is detected.

However, no device is flawless. The consequences of a false alert can seriously affect a patient's security and health. When a false positive alert occurs, a doctor can either call the patient to confirm or send an ambulance right away. Both of these actions can expose private health records to bystanders. If an unexpected ambulance is sent, it would announce a patient's poor health history to those around them. While an IoT monitor enables rapid response times from

---

[22] Chouffani, R. (2016, September). Five challenges of IoT in healthcare that put it at risk of failure. Retrieved from https://searchhealthit.techtarget.com/tip/Five-challenges-of-IoT-in-healthcare-that-put-it-at-risk-of-failure

[23] Spitzer, J. (2018, August 28). Fitbit has logged 150B hours of heart data and 8 other things to know. Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/fitbit-has-logged-150b-hours-of-heart-data-and-8-other-things-to-know.html

[24] Patel, N., Patel, P., & Patel, N. (2018, April). Heart Attack Detection and Heart Rate Monitoring Using IoT. 7. 611-615.

healthcare providers, there is a risk that the patient's healthcare information could be exposed. To reduce the chance of a false positive, the alert threshold can be increased; however, this could lead to dire consequences. A false positive may violate confidentiality, but a false negative could lead to death or injuries.

Along with health records, the personal privacy of users is also at risk. By aggregating seemingly trivial data, it is possible for sensitive information to be exposed, such as a user's location. For example, if a heart rate monitoring device logs an elevated heart rate every work day at 5:30 pm, an adversary can infer that the user is exercising at a location 30 minutes away from work. By incorporating more data, such as daily traffic conditions, locations suitable for exercise, the user's specific location can be narrowed down. While this example may seem far-fetched, data aggregation has already been used to draw important information out of trivial data in other industries. Using information such as zip codes, birth dates, and gender, 87% of individuals can be identified.[25] The increased spread of IoT devices will provide a new source of data that can be used to compromise confidentiality and privacy.

Connected Devices and Integrity

The operation of connected devices is dependent on the accuracy of the data that it collects. Compromising the integrity of this data can result in serious consequences, such as misdosing. In an article published by the Catholic University of Leuven, researchers were able to identify communication protocol flaws with cardiac defibrillators. This flaw enabled them to conduct replay attacks, allowing them to force the device to repeat an action. They also discovered a lack of integrity and authentication checks, enabling attacks in which forged commands are obeyed by the device.[26] Essentially, these attacks enable an adversary to issue arbitrary commands to the defibrillator by compromising the integrity of its communications. This can result in direct harm to the patient, as attackers can turn off or reconfigure the device to prevent or provide cardiac shocks at the wrong time.

Cardiac defibrillators are only one of many devices vulnerable to attacks on integrity. Indeed, researchers at Carnegie Mellon University was able to maliciously recalibrate insulin pumps after exploiting a weakness caused by the device's Bluetooth connection.[27] While insulin pumps are functionally different from cardiac defibrillators, the impact of a successful exploit is the same.

---

[25] McCord, G. (2015, May 05). Choose Privacy Week 2015: What You Should Know About "Anonymous" Aggregate Data About You. Retrieved from https://chooseprivacyeveryday.org/choose-privacy-week-2015-what-you-should-know-about-anonymous-aggregate-data-about-you/

[26] Marin, E., Singelée, D., Garcia, F. D., Chothia, T., Willems, R., & Preneel, B. (2016, December). On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (pp. 226-236). ACM.

[27] Hensler, C., Rogers, J., & Yu, J. (n.d.). *BioT: A Security Assessment of Continuous Glucose Monitoring Systems*[Scholarly project]. Retrieved April 29, 2019.

Connected Devices and Availability

Availability is an important security principle for medical IoT devices, as it can impact whether or not patients receive critical treatments. IoT device manufacturers and their ability to continue operations greatly affects the availability of their devices. In 2016, 15,033 companies filed for chapter 7 bankruptcy protection in the United States.[28] The collapse of a device manufacturer producing connected devices for the healthcare industry is particularly concerning. If a manufacturer is no longer in business, patches will no longer be deployed and could leave users with vulnerable devices. In this scenario, it would be unsafe to use these devices, thus compromising their availability. To make matters worse, replacing embedded devices can be invasive and may require surgery. Without access to a replacement, users may have to rely on vulnerable devices or no devices at all for a period of time.

Security Concerns for Wearable Devices and Bluetooth

Internet-connected hearing aids can greatly improve their existing functionality. These functionalities can include detecting Bluetooth-enabled doorbells or outside of the normal range and, hypothetically, real-time translation to help users communicate in a foreign country.[29] Generally, these devices utilize Bluetooth to connect to other smart devices, which results in a shorter transmission range.[30] In contrast to a wireless internet connection, Bluetooth's shorter transmission range makes it more challenging for an attacker to exploit the device. However, this technology is still susceptible to unauthorized remote access. Currently, a weakness within Bluetooth allows attackers to remotely obtain encryption keys. This weakness may allow attackers to obtain private information or transmit malicious signals to the device.[31]

Expanding the features of traditional hearing aids can improve the quality of life for patients, but it will have a corresponding increase in the attack surface. A concern for connected hearing aids is the potential for malicious actors to eavesdrop on the connection. The sound picked up by the device can be relayed to a 3rd party. There are few tangible benefits to transmitting this data outside of the device, as a connected hearing aid can function without the ability to transmit externally. While this will reduce the risk of attacks it cannot eliminate them completely.

---

[28] National Bankruptcy Forum. (2017, December 14). How many people filed for bankruptcy in 2016? - NBF. Retrieved from https://www.natlbankruptcy.com/how-many-people-filed-for-bankruptcy-in-2016-2/

[29] Carman, A. (2016, June 23). A connected hearing aid is an Internet of Things device I can get behind. Retrieved from https://www.theverge.com/circuitbreaker/2016/6/23/12015076/hearing-aid-connected-internet-smart-internet-of-things

[30] Cashin-Garbutt, A. (2018, July 12). Internet-connected smart hearing aid: A life changing solution? Retrieved from https://www.news-medical.net/news/20170712/Internet-connected-smart-hearing-aid-a-life-changing-solution.aspx

[31] Bluetooth implementations may not sufficiently validate elliptic curve parameters during Diffie-Hellman key exchange. (2018, July 23). Retrieved from https://www.kb.cert.org/vuls/id/304725/

In addition to confidentiality risks, connected hearing aids can also have integrity concerns. In the name of convenience, hearing aids can be connected to electronic gadgets such as laptops and TVs, but these connections expose the device to further attacks. An adversary can potentially replay or modify the signal received by the device through weaknesses within Bluetooth communication.[32] This allows the attacker to manipulate a conversation and extract information from the user. These replay attacks can be leveraged to manipulate the user of the device. For example, they could force the user to leave a location by replaying an evacuation command. Connecting hearing aids to a network expands the attack surface, providing adversaries with more avenues to exploit the user.

Connected Devices and National Security

While the threat of connected medical devices can be damaging to individuals, adversaries can use the same attack vectors to impact national security. Specifically, these connected device attacks can be tailored to target key individuals within the US government. With an average age of 61 years old, the US Congress represents a demographic most likely to require the use of embedded medical devices.[33] This creates opportunities for attackers to target specific policymakers. For example, defibrillator communication protocol flaws can be used to deliver electrical shocks, which an attacker can exploit to impede or coerce a policymaker's influential decisions. In this case, the democratic process could effectively be compromised.

Individual privacy concerns may also pose as a national security issue when data are aggregated. Using data collected by fitness devices such as Fitbit, Strava created a global heat map of user locations over a 2 year period. In active war zones, this map revealed a concentration of users in known and previously unknown military bases.[34] As more healthcare devices connect to the internet, data aggregation can reveal further information on sensitive locations.

Connected Devices and Security Posture

Many of the security vulnerabilities related to IoT devices apply to all industries, but the impact of an attack is more pronounced if it occurs in the healthcare industry. The healthcare industry is a custodian of unique assets such as health records. These information security risks are correlated with the organization's security posture. A stronger security posture mitigates risk

[32] Bluetooth implementations may not sufficiently validate elliptic curve parameters during Diffie-Hellman key exchange. (2018, July 23). Retrieved from https://www.kb.cert.org/vuls/id/304725/

[33] King, K. (n.d.). The 115th Congress is among the oldest in history. Retrieved from https://www.quorum.us/data-driven-insights/the-115th-congress-is-among-the-oldest-in-history/175/

[34] Sly, L. (2018, January 29). U.S. soldiers are revealing sensitive and dangerous information by jogging. Retrieved from https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?noredirect=on&utm_term=.454013e1c229

with preparedness. The value of these assets in the organization and the poor security environment create a challenge for securing IoT devices in the healthcare industry.

As noted before, the healthcare industry is not equipped to handle existing security threats. In the hierarchy of design, functionality will always be more important. Traditionally, this has led to security being considered as an afterthought.[35] Combined with the increasing attack surface created by the incorporation of IoT devices, there will be more potential vulnerabilities in the future. To mitigate this security risk, additional funding will be required for device patch management, configuration and implementation. For devices that leave the network, additional funding is needed to secure the device. At the same time, manufacturers can implement security within their development cycle. These are not one-time expenses, as the cost to secure these devices will persist for the lifetime of the device. As the industry currently stands, connected devices can stretch the ill-equipped security safeguards to their breaking point and worsen the problems. Furthermore, not all devices should become network enabled, connecting these devices may compromise security without providing tangible benefits for the patients. In the end, the risks of using IoT devices can be addressed with improving security postures, but healthcare providers should seek to balance the benefits and risks of connected devices before connecting devices to the network.

The Effect of Supply Chain Attacks for the Healthcare Industry

A further issue that the healthcare industry will face in the future is related to supply chain vulnerabilities. These vulnerabilities can be significant as attacks that leverage them circumvent many traditional security strategies. These vulnerabilities can occur in both hardware and software. In hardware, the device is compromised prior to the company receiving the device. In software, the application can be compromised in different stages of the software development life cycle. For instance, it can occur during the maintenance phase, in which applications are not patched to address critical security issues or used to install malicious software instead.

Supply Chain Vulnerability Overview

Connected devices are only one component of the healthcare system that faces security risks. Another potential attack vector that malicious actors can exploit within the healthcare industry is the supply chain. A highly publicized example of this type of vulnerability was published by Bloomberg, which alleged that Chinese spies inserted small hardware implants within computing equipment to compromise private companies.[36] While these allegations have been challenged and their authenticity remains in doubt, the article is significant as it opened the door for a

---

[35] Scanlon, L. (2019, April 23). CMU Interview with Leo Scanlon [Telephone interview].

[36] Robertson, J. & Riley, M. (2018, December 4). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

conversation on supply chain vulnerabilities that was long overdue for both private and public organizations.

These attacks stem from the increasingly complex and difficult to manage process by which physical equipment is manufactured and software is developed. For example, a single computer must travel through several phases while being manufactured and these phases present opportunities for the device to be compromised. The initial compromise can occur when the hard drive is being manufactured, when the components are waiting for assembly, or during the shipping process; only one weak link is necessary to compromise the entire chain. A failure in the supply chain will result in compromised devices that can be used to exploit vulnerabilities within the purchasing organization's secured environment. To further complicate the matter, receiving a compromised device is only one of the many consequences of a supply chain failure. Counterfeit electronics have become increasingly popular and are almost impossible to detect in normal use. These counterfeit electronics may contain inferior components that fail when they are needed the most.

Supply chain vulnerabilities are also not exclusive to hardware. Similar problems exist for software as well. Software development is not done in a vacuum, and developers often utilize pre-existing software libraries to prevent duplicating work and to reduce the use of resources during the development process. However, vulnerabilities in key software libraries can cascade down to dependent applications, increasing the attack surface. In this case, security patches will be needed to prevent potential exploitations. The software development life cycle also does not end at the development stage, as deployment, maintenance, and the patching of software can also introduce additional vulnerabilities. For example, if the update server is compromised, an adversary can deploy poisoned updates to attack organizations that utilize the software.

Examples and Potential Impact

These scenarios may seem far-fetched, but there have been examples of supply chain vulnerabilities across a multitude of different industries. In one instance, a malicious actor was able to install malware onto newly manufactured barcode scanners in China. The malware was designed to send all scanned data, including source and destination addresses, to a location in China. This ultimately compromised the company's network and allowed attackers to exfiltrate confidential proprietary information, such as financial and shipping data.[37] With the equipment compromised during the manufacturing process, companies were unaware of the infection. Once activated, the malware enabled malicious actors to penetrate secured networks and issue arbitrary commands.

[37] (2017). Zombie Zero: Weaponized Malware Target ERP Systems. *TrapX Security*. Retrieved from http://www.trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf

These types of attack have occurred within the healthcare industry as well. In one incident, the American Dental Association sent 37,000 USB drives to its members which were infected during the manufacturing process.[38] These USB drives were meant to contain updated dental procedure codes, which are used to track procedures for insurance purposes. Since they would likely be plugged into the billing system, these infected USB drives would have access to personally identifiable information (PII). While physical access is necessary, the technical barrier to perpetrating such an attack is minimal. Compromised USB drives can be purchased online for as little as $50, and software tools to make your own batch of infected drives are freely available on Github.[39] A security incident may not only affect the organization's reputation, but also prevent medical professionals from providing patient care. Sequentially reducing the productivity and quality of care that the organization can provide.

To place these types of attacks in the context of national security, compromised devices could be used in healthcare and other types of critical infrastructure. The potential for backdoors is evident if a nation state invests resources and deploys their equipment to other countries. For example, the telecommunications industry is currently in the process of deploying 5G cellular infrastructure. 5G cellular technology promises to provide more bandwidth, low latency, and high reliability, which can revolutionize connected devices.[40] However, the US has raised concerns with utilizing equipment provided by Huawei, a Chinese telecommunications company with purported strong ties to the Chinese government, for 5G deployment.[41] According to their claims, Huawei has the potential to implement backdoors and provide sensitive information to the Chinese government.

From a national security perspective, relying on a foreign nation's infrastructure to operate critical systems opens the possibility for a failure with catastrophic consequences. To place these concerns in a healthcare environment, the deployment of 5G technology and the evolution of cellular capabilities can result in big changes to patient care. Providing remote care via live video has allowed patients to get the care they need without having to physically travel to their medical practitioner. 5G, which promises increased bandwidth and decreased latency, will facilitate the continued growth of such care and offer consistent, real-time monitoring of connected devices. If these capabilities were suddenly shut down or if the data was stolen, the consequences for

---

[38] Krebs, B. (2016, April 28). Dental Assn Mails Malware to Members. *Krebs on Security*. Retrieved from https://krebsonsecurity.com/2016/04/dental-assn-mails-malware-to-members/

[39] Smith, M. (2016, June 22). Say hello to badUSB 2.0: a USB man-in-the-middle attack proof of concept. *CSO Online*. Retrieved from https://www.csoonline.com/article/3087484/say-hello-to-badusb-20-usb-man-in-the-middle-attack-proof-of-concept.html

[40] Qualcomm Technologies Inc. (2016, February) Leading the World to 5G [Powerpoint Slides]. Retrieved from https://www.qualcomm.com/media/documents/files/qualcomm-5g-vision-presentation.pdf

[41] Washington Post Editorial Board. (2019, April 02). U.S. allies should heed the warnings about Huawei. *The Washington Post*. Retrieved from https://www.washingtonpost.com/opinions/global-opinions/huawei-wants-the-governments-trust-a-new-report-advises-caution/2019/04/02/5a1c7e5a-54b2-11e9-814f-e2f46684196e_story.html?noredirect=on&utm_term=.dac9f87e58b3

patients and the nation as a whole would be dire. Even if these concerns are not realized, critical infrastructure sectors need to be aware of the threats faced from using controversially-sourced technology.

Supply chain vulnerabilities can also be leveraged to subtly attack organizations. When purchasing hardware and computer equipment, it is possible for an organization to receive products with inferior or counterfeit components. The US Department of Defense has flagged counterfeit electronics as a serious risk to national security, as these components may be of lower quality or contain known vulnerabilities, providing footholds for hackers or crashing a critical system.[42] This a significant concern for any healthcare organization as counterfeit parts are difficult to detect and patients would be significantly impacted if the counterfeiting made its way to medical devices. Decreased performance or unexpected shutdowns in such devices could result in serious injury. With hardware being a major component within the healthcare system, an exploited supply chain vulnerability can manifest itself in many ways to affect every aspect of the healthcare industry.

To extend beyond hardware exploits, there are examples of software being compromised in the same way. Applications that are purchased or available for free online are often closed-source, which means that the source code cannot be viewed or audited by anyone but the developers. Without access to the source code, customers are more vulnerable to supply chain vulnerabilities as they must presume that the software is both functional and secure. Even if an open-source application is shown to be vulnerable, having access to the source code means that security patches could be written to address the problem. This is not a perfect solution to the issue and there are reasonable justifications to avoid open-source software, but relying on a single company to provide all of the required support and patching is not ideal.

Having a single point of failure, which can occur if the company chooses to drop support or goes out of business, is not an effective defensive strategy. One example of this refers to the patching phase of application development. The increasing complexity in software development requires application developers to constantly patch newly discovered vulnerabilities. These updates can become vulnerabilities as the users have no way of verifying the security of these patches. Malicious actors can compromise the update servers to poison updates and inject malware into the users' systems. Upon execution, the end users have unknowingly installed a malicious payload, thus compromising their systems.

Several incidents of poisoned updates have already been recorded in other industries. In 2017, legitimate sysadmin software downloaded and installed a Trojan backdoor from a compromised

[42] U.S General Accountability Office (2012, May 21). Inquiry into counterfeit electronic parts in the department of defense supply chain. *Committee on Armed Services US Senate*. Retrieved from https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

server during the update process.[43] This backdoor gave attackers the ability to view and modify confidential data and shut down key services. In 2014, a fast breeder reactor facility in Japan noticed that staff emails and training documents were being exfiltrated.[44] This stemmed from an update for the free media software, GOM player, which had installed a malicious payload during its attempt to update. Another incident occurred on March 25, 2019, when consumers who purchased computers and motherboards manufactured by ASUS were notified that the ASUS LiveUpdate tool had been compromised. In this incident, hackers were able to push digitally signed infected patches onto their devices, compromising ASUS consumers' personal devices.[45]

Poisoned update attacks are not new nor are they specific to any industry. These attacks do not require significant technical skills and they can be utilized against healthcare organizations to compromise systems en masse. Due to the value of PII on the black market and the heightened reliance on information technology, the healthcare industry should be aware of these types of attacks going forward.

Emerging Technology

Technological innovations such as artificial intelligence, data analytics, and cloud computing have revolutionized healthcare processes. Many of these same emerging technologies can also be used to prevent and/or detect threats and attacks aimed at disrupting the healthcare industry. The promise of these technologies in providing advanced cyber security capabilities has led to extensive research and investment from both the private and public sectors. In the following section, this paper will discuss how emerging technologies can be leveraged by healthcare organizations to mitigate the many cyber threats they face.

The Role of Artificial Intelligence and Machine Learning in Cyber Security

Artificial intelligence (AI) is a technology that allows computers to learn from experience, enabling them to perform human-like tasks. Computers can be trained to perform specific tasks and make decisions based on data analysis and pattern recognition.[46] Their autonomous behavior, high-speed accuracy, intelligent decision making, and analytics can also be utilized to develop information security tools.[47] Sophisticated AI-enabled firewalls with faster multi-vector threat

---

[43] RSA. (2017). Kingslayer: a supply chain attack. *IT Worlds Media*. Retrieved from https://www.itworldsmedia.com/admin/whitepapers/kingslayer---a-supply-chain-attack.pdf

[44] Graham, M. (2014, February 19). Context threat intelligence - the monju incident. *Context*. Retrieved from https://www.contextis.com/en/blog/context-threat-intelligence-the-monju-incident

[45] (2019, March 25). ShadowHammer: Malicious updates for ASUS laptops. *Kaspersky*. Retrieved from https://usa.kaspersky.com/blog/shadow-hammer-teaser/17396/

[46] Artificial Intelligence – What it is and why it matters. (n.d.). Retrieved from https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html

[47] Elsa Kania, D. P. (2019). *Translation: Key Chinese Think Tank's "AI Security White Paper" (Excerpts).* https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-key-chinese-think-tanks-ai-security-white-paper-excerpts/

detection can reduce the occurrence of data breaches by limiting information leakage and identifying the source of the information leak. This technology is particularly valuable in the healthcare industry, as it can serve to protect sensitive patient data (e.g., EHRs). [48]

A branch of AI that involves creating algorithms that facilitate machines to learn from training data(data set used to train models to perform activities) and make intelligent decisions is called Machine Learning (ML). This concept can be used in defensive security tools that can flag malicious activities faster by making decisions based on similar pattern behavior in training data set fed into it. Furthermore, making a machine be able to make cognitive decisions just like the human brain, an artificial neural network that mimic the functioning of neurons in the brain usually referred to as Deep Learning (DL) is currently being implemented in medical devices like MRI and CT scanners for efficient diagnostic purposes.

Apart from defensive security, emerging technology can help in assessing risk in an accurate manner. It provides improved efficiency and accuracy to risk assessments when integrated with such risk management frameworks. With its wide range of applications, it can definitely create a positive impact to the current security posture of healthcare.

Use Cases

Due to the increased risk of sophisticated cyber attacks, public and private institutions are investing in developing new tools that help combat healthcare related cyber issues. AI and ML based solutions are one such technology that these organizations are focusing their research and development into, as they have the potential to mitigate many of the risks that new cyber threats offer. Companies have already released and in the process of releasing products that perform activities ranging from preventing and detecting malicious activities to detecting specific threat actors like insider threat.

Focusing on preserving data confidentiality, a robust application of AI/ML in firewall tools can improve detection rate by more than 60%. There products when integrated with cloud services enabled the AI to exchange information and learn about current threat, threat actors, and provide good cyber hygiene practices. [49]

Another strategy that can greatly benefit from AI/ML integration is on threat prevention at the network endpoint. Unlike traditional antiviruses, where the system compares hashes and binaries to known malicious signatures, AI/ML can learn from previous samples of malware and perform

[48] Elsa Kania, D. P. (2019). Translation: Key Chinese Think Tank's "AI Security White Paper (Excerpts). *New America*. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-key-chinese-think-tanks-ai-security-white-paper-excerpts/.

[49] (2019). Don't let healthcare cybersecurity threats limit your ability to deliver and improve care. *IBM*. Retrieved from https://www.ibm.com/industries/healthcare/cybersecurity

behavioral analysis for detection. Even if the malware is modified or improved, the AI model would be able to adapt by identifying new behaviors for detection.
Furthermore, the technology can be scalable on everything from small IoT devices to large supervisory control and data acquisition (SCADA).[50] According to Malcolm Harkins, Chief Security and Trust Officer at Cylance, this process allows AI/ML based solutions to offer some protections against advanced and zero-day attacks[51]. He also mentioned about ML enabled products that read user keystrokes and automatically identify keystrokes of unauthorized users. This can greatly benefit any healthcare sector vulnerable to insider threats.[52] With the current environment in mind, integrating AI/ML with existing software tools can serve to expand their functions and capabilities.

Role of Blockchain in Cyber Security

Blockchain is a peer-to-peer ledger-based technology,[53] which consists of blocks of digital data stored in a decentralized public database. It provides transparency, as any changes made to the ledger are recorded and can be easily traced back. Each block has a unique hash that is generated each time data is added to them. If these blocks need to be modified, a majority of the blocks or parties involved must give consent before it is accepted.[54] This provides an advantage over a traditional centralized database as modifications must be agreed upon, decreasing the chances for a malicious actor to compromise the data within.

This technology has the potential to be used in the healthcare sector to keep patient data safe and secure by utilizing its ability to provide uninterrupted and transparent logs of patient data. Use of a private blockchain helps to authorize the users accessing the blockchain and lowers the risk of being a successful attack.[55] The decentralized nature helps to share data among various health sectors quickly and safely.

To provide an example of how blockchain can be implemented to provide cyber security in primary patient care, considering the scenario where patients need to consult with different hospitals. It can be difficult and time-consuming to transfer patient medical history from one hospital to another in a secure manner. If a private blockchain were to be set up with only trusted peers (hospitals, relatives and pharmacies) allowed to maintain the ledger, a user will be able to

---

[50] Mullen, M. (2018, August 23). Critical Infrastructure. *BluVector*. Retrieved from https://www.bluvector.io/industry/critical-infrastructure/
[51] Harkins, M. (2019, April 18). CMU Interview with Malcolm Harkins [Telephone interview].
[52] Harkins, M. (2019, April 18). CMU Interview with Malcolm Harkins [Telephone interview].
[53] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2018, April 16). Secure and Trustable Electronic Medical Records Sharing using Blockchain. *National Institutes of Health*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/
[54] Fortney, L. (2019, February 10). Blockchain, Explained. *Investopedia*. Retrieved from https://www.investopedia.com/terms/b/blockchain.asp
[55] Binani, H. (2019, February 11). Blockchain in Healthcare : A Case for Innovations & Opportunities. *Cuelogic*. Retrieved from https://www.cuelogic.com/blog/blockchain-in-healthcare

access and manage the data through one of the nodes blockchain network. The private blockchain provides key management and access control policy that is encoded into the network thus ensuring security and privacy.[56]

Future Innovations

Artificial intelligence is still evolving and hence there are many companies investing in research projects related to implementing it in cyber security. Fully Homomorphic Encryption (FHE) is one such technology to provide secure analytics and monitoring of personal health records. It can prevent data breaches by providing encryption to data-at-rest and data-in-transit. When encrypted personal health information stored in databases is queried, FHE encrypts the query before execution and returns an encrypted output. The answer can then be decrypted on a trusted platform.[57]

A cloud service that is becoming popular is "Disaster Recovery-as-a-Service (DRaaS)", which provides data backups and resumption of business operations. It helps to provide business continuity and resiliency during and after a significant system failure. Consolidating services to one entity allows the industry to reduce overhead cost. Some cloud services also allow organizations to use cryptographic keys to secure private data that they upload, which keeps data that is stored in a cloud to be kept private from the cloud service provider. However, these services can create a single point of failure and can be targeted by attackers.[58]

Risks of Using Advanced Technology

Emerging technologies and underlying decision-making models are complex and can be difficult to understand. Hence, even if a violation is detected, it might be ignored or interpreted incorrectly. Implementing AI based security tools in organization can lead to a new set of vulnerabilities while the model is being developed, trained, and configured. (Ryan Goosen, 2018). Furthermore, attackers can use AI to automate their attack vector enabling them to launch attacks faster, in a short time and with less cost. Research has revealed its use in automated social engineering attacks like phishing campaign that could easily bypass an AI enabled detection mechanism (Newman, 2018). There are also evidences of AI being used for this purpose and we will be exploring a new of such techniques.

---

[56] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2018, April 16). Secure and trustable electronic medical records sharing using blockchain. *National Institutes of Health*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/

[57] Archer et al,. (2017). Applications of homomorphic encryption. Retrieved from http://homomorphicencryption.org/white_papers/applications_homomorphic_encryption_white_paper.pdf

[58] Technopedia. (n.d.). What is disaster recovery as a service (DRaaS)? - definition from technopedia. Retrieved from https://www.techopedia.com/definition/29773/disaster-recovery-as-a-service-draas

Adversarial machine learning attacks are attacks that target the learning model to cause a malfunction. There are 2 types of such attacks. Poisoning attacks involve online learning ML models where attacker provides faulty data that redirects the decision boundary in his or her favor, and evasion attack where attacker modifies the model to misclassify a sample of data. These attacks can be used against the picture archiving and communication systems (PACS) which affects CT and magnetic resonance imaging (MRI) scan results.[59]

Leo Scanlon, a senior advisor for Healthcare and Public Health Sector Cybersecurity at the U.S. Department of Health and Human Services (HHS) talks about AI based algorithms used by attackers during his presentation at a Health TechNet event. He mentions generative adversarial network (GAN) a type of machine learning algorithm that have been successful in password cracking. PassGAN is a tool that was tested against other password cracking tools like John the Ripper and HashCat."The GAN was remarkably successful: It was trained on 9.9 million unique leaked passwords — 23.7 million including duplicates — which represented real human output."[60] Traditional brute force mitigations include identifying non-human behavior, such as attempting a database of passwords multiple times per second. This machine learning approach to breaking passwords presents a threat to current password security standards.

CT scanners have provided significant benefits to the medical industry, but these devices can also be vulnerable to attacks. Researchers from Ben-Gurion University Cyber Security Research Center were able to create malware that uses deep learning (DL) that could modify CT scans. This malware allowed the researchers to automatically add or remove malignant growths to lung scans. When they were unaware of the virus, 3 radiologists failed to detect the alterations 99 and 94 percent of the time for growth fabrication and removal, respectively. Once aware of the experiment, they were still unable to detect the alterations 60 percent of the time.[61]

The removal of malignant growths in scanned imaging can have damaging effects on patients. Timely treatment is key to cancer treatments. The modified image can delay or deny patients life-saving medication or procedures. While this is concerning, the malware requires the intruder to be on the network and will not work if the images were digitally signed or encrypted. Ideally, these mitigations should be already in place to add extra layers of protection. However, the systems involved in this attack are frequently unencrypted. Even when the systems were encrypted, researchers were still able to compromise the communication due to security

---

[59] Scanlon, L.(2019, March). Artificial intelligence: and what is it? security challenges when models behave badly [Powerpoint Slides].

[60] Scanlon, L.(2019, March). Artificial intelligence: and what is it? security challenges when models behave badly [Powerpoint Slides]

[61] Zetter, K. (2019, April 03). Hospital viruses: fake cancerous nodes in CT scans, created by malware, trick radiologists. Retrieved from https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?noredirect=on&utm_term=.dcdb648a7ad8

misconfigurations.[62] While encryption offers strong protections, it cannot be the only source of mitigations.

Another scenario about how emerging technology could have been used to influence the 2016 presidential election, there were concerns for Hillary Clinton's health.[63] While these rumors can be easily dismissed with medical examinations, modified reports could feed the rumors. With the malware developed to modify CT scans, both doctors and patients can be tricked into a false cancer diagnosis. For a presidential race, serious medical conditions can have a negative impact on their electability. In this scenario, the attacker can manipulate election results by using medical records to compromise the integrity of the country's democracy.

As mentioned earlier, blockchain could potentially transparency of healthcare transactions but it can also be used for malicious purposes. Christian Karam, a speaker at BlackHat Asia conference talks about blockchain being used to store malware control mechanisms and illicit content that would be hard to remove.[64] In order to demonstrate blockchain based attacks, researchers at United Kingdom's University of Newcastle created "Zombiechain" a command and control botnet that can send instructions to malware on a bitcoin network.[65]

Healthcare Industry – A Policy Perspective

The internet boom of the 1990s revolutionized the healthcare industry, as many within the industry saw the advantages to modernizing healthcare information – namely the creation of EHRs. However, this technological change came with the need for stricter privacy and security protection requirements. Since the 1990s, EHR protection has been largely facilitated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[66] Although HIPAA covers the protection and security aspect of EHRs, it was primarily designed to address employee health insurance coverage in between jobs – not network security. This important detail highlights one of the many reasons why healthcare organizations often fall victim to cyber-crimes. Simply put, many hospitals lack substantive security policies and frameworks to aid in cyber incident prevention and mitigation.

---

[62]Zetter, K. (2019, April 03). Hospital viruses: fake cancerous nodes in CT scans, created by malware, trick radiologists. Retrieved from https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?noredirect=on&utm_term=.dcdb648a7ad8

[63]Zetter, K. (2019, April 03). Hospital viruses: fake cancerous nodes in CT scans, created by malware, trick radiologists. Retrieved from https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?noredirect=on&utm_term=.dcdb648a7ad8

[64] Fox-Brewster, T. (2015, March 28). Bitcoin's Blockchain Offers Safe Haven For Malware And Child Abuse, Warns Interpol. Retrieved May 06, 2019, from https://www.forbes.com/sites/thomasbrewster/2015/03/27/bitcoin-blockchain-pollution-a-criminal-opportunity/#4145eedb207b

[65] WASSERMAN, T. (2018, March 16). The intersection of technology, innovation & creativity. Retrieved May 06, 2019, from https://now.northropgrumman.com/blockchain-technologys-dark-side-worries-department-defense/

[66] Office for Civil Rights. (2013). Summary of the HIPAA security rule. *U.S. Department of Health and Human Services.* Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

In 2018, 351 data breaches involving at least 500 healthcare records were reported to the Department of Health and Human Services' Office for Civil Rights. Of the 351 reported cases, 18 incidents resulted in the exposure of over 100,000 patient records. The primary cause for these breaches was linked to "Hacking/IT incidents", which details either a lack of effective security measures, insufficient cyber hygiene, or both.[67] According to a 2016 report by the Healthcare Information and Management Systems Society, 52% of U.S. hospitals use connected health technologies and by 2021 the use of these devices is expected to grow by 26%.[68,69] Not only will new medical technology work to revolutionize the patient experience, but it will also pose new problems by increasing the attack surface for many healthcare organizations.

Policies & Frameworks as a Mitigating Solution

Implementing a cybersecurity-focused framework in addition to information security policies and procedures is an effective way to combat many of the issues new technologies bring to an organization. Additionally, cybersecurity frameworks help simplify this complex field while being cost-effective, flexible, and auditable.[70] For an industry filled with resource-strapped organizations, such as hospitals, these frameworks serve as important guidelines to improve privacy and security controls. However, finding the right framework can be difficult. An appropriate framework should not only protect the confidentiality, integrity, and availability of healthcare assets, but also work to maintain HIPAA compliance – a critical concern for many healthcare organizations.

In order to better understand which framework would best fit the healthcare model, it is important to understand where the weak links are. A 2018 Abbott and The Chertoff Group report found that over 90% of physicians and hospital administrators believed that data security is a focus of their hospital. However, 75% of physicians and 62% of administrators felt "inadequately trained or prepared to mitigate cyber risks that may impact their hospital".[71] It is clear that healthcare leaders understand the importance of mitigating cyber threats; they are just not confident on how to do it.

---

[67](2018, December 27). Largest healthcare data breaches of 2018. *HIPAA Journal*. Retrieved from https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/

[68] Siwicki, B. (2016, March 2). 52% of US hospitals use 3 or more connected health technologies, HIMSS study finds. *Healthcare IT News*. Retrieved from https://www.healthcareitnews.com/news/52-us-hospitals-use-3-or-more-connected-health-technologies-himss-study-finds

[69] Markets and Markets (2016, October 20). Medical device connectivity market worth 1,344.1 million USD by 2021. *Cision PR Newswire*. Retrieved from https://www.prnewswire.com/news-releases/medical-device-connectivity-market-worth-13441-million-usd-by-2021-597767741.html

[70] Lohrmann, D. (2018, May 20). Why you need the cybersecurity framework. *Government Technology*. Retrieved from http://www.govtech.com/blogs/lohrmann-on-cybersecurity/why-you-need-the-cybersecurity-framework.html

[71] Abbott and The Chertoff Group. (2018, November 15). Abbott and the Chertoff group explore current state of cybersecurity in the connected hospital. *Abbott.* Retrieved from https://abbott.mediaroom.com/2018-11-15-Abbott-and-The-Chertoff-Group-Explore-Current-State-of-Cybersecurity-in-the-Connected-Hospital

The lack of cyber hygiene, training, and awareness is especially disconcerting as healthcare facilities are often the prime targets for malware attacks, especially ransomware. While backups of critical records are recommended as a mitigating strategy for ransomware, it is often not an effective strategy for healthcare facilities. Often, the redundancy time needed to recover the records can take up to weeks. In an industry where minutes and hours can mean the difference between life and death; that is simply not an option. This was the case for Hancock Health, a healthcare facility in Indiana which paid a $55,000 ransom to unlock their records. Although Hancock had up-to-date backups to recover their data, it was faster to pay the ransom than to utilize the backups. Hancock's breach was ultimately a result of compromised third-party vendor credentials; however, more robust network segmentation and least privilege policies, aspects found in effective cybersecurity frameworks, could have mitigated the attack.[72] Cybersecurity framework adoptions can help healthcare facilities enumerate relevant assets and ensure they have robust controls in place that are commensurate with the security industry's best practices.

Cybersecurity Frameworks – A Comparison

Of the cybersecurity frameworks currently in use, most healthcare organizations are turning to the NIST Cybersecurity Framework (CSF) v.1.1 and the HITRUST framework.[73] According to the 2018 HIMSS Cybersecurity Survey, 57.9% of organizations have adopted the NIST CSF and 26.4% of organizations adopted the HITRUST framework (Fig. 3).[74] There are a number of reasons why these two frameworks have traditionally dominated the healthcare industry.

Framework	N	percent
NIST	**103**	**57.9%**
HITRUST	47	26.4%
Critical Security Controls	44	24.7%
ISO	7	18.5%
COBIT	13	7.3%
Other	9	5.1%
No security framework has been implemented at my organization	30	16.9%
Don't know	15	8.4%

Fig. 3 2018 HIMSS Cybersecurity Survey framework adoption (HIMSS, 2018)

[72] Osborne, C. (2018, January 17). US hospital pays $55,000 to hackers after ransomware attack. *ZD Net*. Retrieved from https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/

[73] (2019). Healthcare's most wired: national trends 2018. *The College of Healthcare Information Management Executives*. Retrieved from https://chimecentral.org/wp-content/uploads/2018/10/Healthcares-Most-Wired%E2%80%94National-Trends-2018-FINAL.pdf

[74] Healthcare Information and Management Systems Society. (2018). 2018 HIMSS Cybersecurity Survey. *HIMSS*. Retrieved from https://www.himss.org/2018-himss-cybersecurity-survey

First, and perhaps most noticeably, full implementation of the HITRUST framework can cost an organization between $40,000 and $250,000 per year, depending on assessment results. This can be a deciding factor for healthcare organizations working under tight budgets.[75] The NIST framework, on the other hand, is completely free and can be accessed by any organization interested in improving their security posture. Second, a key benefit to the HITRUST framework is that it was designed specifically for the healthcare industry. HITRUST's board of directors consist of healthcare industry executives, who would be most well-suited to understand the technological and privacy challenges healthcare organizations face.[76] Although the NIST CSF was not designed explicitly for the healthcare industry, the Office for Civil Rights designed a healthcare crosswalk to map NIST to HIPAA's key security requirements.[77] Lastly, the NIST framework was designed to be easy to adapt and capable of protecting the US government's critical infrastructure.[78] For these reasons, it is regarded highly in the cybersecurity domain and is often an easy choice for organizations looking to improve their security practices. Ultimately, healthcare organizations must first recognize the need for a systematic approach to security before they can compare frameworks to determine which one will best meet their security needs.

Cybersecurity frameworks are not only designed for healthcare facilities handling sensitive data, they can also be used as mitigating strategies for medical device manufacturers. In 2018, the FDA and The MITRE Corporation collaborated on a Medical Device Cybersecurity Playbook. The Playbook leverages the NIST framework's five main pillars: Identify, Protect, Detect, Respond, and Recover (Fig. 4), and is designed to give manufacturers and healthcare organizations a tool to address "cybersecurity threats affecting medical devices that could impact continuity of clinical operations for patient care and patient safety."[79,80]

---

[75] Pierce, R. (2018, September 26). What is HITRUST? A practical guide to certification. *Lindford & Co.* Retrieved from https://linfordco.com/blog/what-is-hitrust/

[76] (n.d.). HITRUST board of directors. *HITRUST*. Retrieved from https://hitrustalliance.net/about-us/board-directors/

[77] Office for Civil Rights. (2016, February 23). Addressing gaps in cybersecurity: OCR releases crosswalk between hipaa security rule and nist cybersecurity framework. *Health and Human Services*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html

[78] (2018, April 16). Framework for improving critical infrastructure cybersecurity. *National Institute of Standards and Technology*. Retrieved from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[79] (2018, April 16). Framework for improving critical infrastructure cybersecurity. *National Institute of Standards and Technology (NIST)*. Retrieved from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[80] MITRE. (2018, October). Medical device cybersecurity: regional incident preparedness and response playbook. *The MITRE Corporation*. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf

Fig 4. NIST CSF Five Pillars (NIST, 2018)

Many of the largest medical device manufacturers have well-established and strong security programs in place. Medtronic, arguably the largest medical device manufacturer (MDM) in the world, incorporates the NIST CSF and ISO 27000 standards and works with security researchers to address medical technology risks.[81] With this in place, one might wonder why Medtronic and other MDMs continue to produce less-than-secure products. Oftentimes, this stems from three main issues:

1. Medical devices often lack strong security features, such as encryption, because they can make medical devices less efficient. For example, the battery life of devices that encrypt data in transit and at rest can be negatively impacted. However, encrypting data ensures the integrity and confidentiality of sensitive patient information.

2. There is a lack of communication between manufacturers and healthcare facilities regarding asset ownership. Who is responsible for the data transmitted and/or stored? Patch management and updates? When the device is no longer operable, who is in charge of storing it and/or its secure destruction? Assessing and assigning asset owners is integral to most cybersecurity frameworks; however, healthcare organizations and manufacturers must ensure that these roles are clearly defined.

3. Security is often an afterthought in the development lifecycle rather than built in by design. Adding a security feature to a device last minute to satisfy a regulation or quickly mitigate a

[81] Medtronic. (2018, July). Product security. *Medtronic*. Retrieved from https://www.medtronic.com/us-en/product-security.html

vulnerability can often lead to mismanaged dependencies and may disrupt a healthcare facility's workflow.[82]

Mitigating Strategies for the Supply Chain

The risks that occur as a result of supply chain vulnerabilities are extremely varied and complete mitigation can require an impractical amount of resources. Given the limited resources available to companies within the healthcare industry and the potentially unlimited resources of the threat community, cybersecurity frameworks are efficient mitigating strategies. Two frameworks are particularly effective in this regard: the NIST CSF and MITRE's Deliver Uncompromised.

The NIST CSF includes a section on supply chain risk management, which mentions drafting formal contracts with vendors (e.g., service level agreements) and routinely assessing suppliers and third-party partners, such as sourcing components and equipment from trusted partners.[83, 84] Some examples for the security assessment of the vendors can include physical deterrents, such as gates, guns, and guards, to software deterrents, such as encryption, network segmentation, and privilege management.

MITRE's "Deliver Uncompromised" contains actionable information and advice on how to secure the supply chain.[85] It includes key recommendations such as establishing a chain of command, accountabilities, and, similar to the NIST CSF, increasing the importance of security when selecting a vendor. Although written for the US Department of Defense, many of its suggestions are just as relevant to the healthcare industry. Specifically, managing supply chain risks is not a characteristic of one industry -- it impacts them all. Utilizing the MITRE or NIST strategies can provide critical guidance to lower the risk of organizational compromise.

Frameworks are a great start for most organizations, but often they need a more comprehensive security approach. According to a 2018 CHIME report, only 29% of healthcare organizations reported that they had a comprehensive program in place. Comprehensive programs include establishing an acceptable security budget, hiring for executive security leadership positions,

---

[82] Williams, P. AH. & Woodward, A. J. (2015, July 20). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *US National Library of Medicine National Institutes of Health*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/

[83] (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology (NIST)*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[84] Baldwin, K. (2018, October 24). Long-Term Strategy for DoD Assured Microelectronics Needs and Innovation for
National Economic Competitiveness [PowerPoint slides]. Retrieved from https://www.acq.osd.mil/se/briefs/2018_21335_Baldwin_MINSEC.pdf

[85] Nissen, C. & Metzger, R. (2018, August). Deliver Uncompromised A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War. *MITRE*. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf

such as a CISO, and creating oversight committees. Creating oversight committees is a particularly low-cost way for healthcare facilities to ensure that they are maintaining security best practices and meeting their security goals.[86] Additionally, including threat-specific programs can also work to mitigate an organization's biggest threats. For healthcare facilities, that threat is on the inside.

Insider Threat Programs

The high degree of internal actors abusing their access to sensitive data illustrates the need for substantive training programs and the implementation of an Insider Threat Program (ITP). According to the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute, an insider threat is "the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization".[87] An ITP is designed to mitigate the risks of these insiders and should be developed for a specific organization based on their business model and needs. For healthcare facilities, their need is to mitigate the risks posed by insiders and their business model requires an option that is resource-friendly. A high-quality ITP can be developed for free or at a very low cost using open-source tools – which satisfies both of their requirements. For example, the National Insider Threat Task Force offers free resources and training material to organizations interested in creating or improving their own programs.[88]

Effective ITPs generally include five categories: User Activity Monitoring (UAM), Data Loss Prevention (DLP), Security Information and Event Management (SIEM), Analytics Tools (to detect anomalous activity), and Digital Forensics Tools (to aid in investigations).[89] The SANS Institute also recommends organizations combine CERT's best practices and Insider Threat components with the NIST Cybersecurity Framework. By implementing CERT's thirteen key components of an Insider Threat program, healthcare facilities can better mitigate one of the largest threat actors they face, their employees.[90]

---

[86] (2019). Healthcare's most wired: national trends 2018. *The College of Healthcare Information Management Executives*. Retrieved from https://chimecentral.org/wp-content/uploads/2018/10/Healthcares-Most-Wired%E2%80%94National-Trends-2018-FINAL.pdf

[87] Costa, D. (2017, March 7). CERT definition of 'insider threat' – updated. *Software Engineering Institute*. Retrieved from https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

[88] Office of the Director of National Intelligence. (n.d.). National insider threat task force (NITTF) mission. *National Insider Threat Task Force*. Retrieved from https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

[89] Silowash, G. (2016, July 26). Building an insider threat program: five important categories of tools. *Software Engineering Institute*. Retrieved from https://insights.sei.cmu.edu/insider-threat/2016/07/insider-threat-program-five-important-classes-tools.html

[90] Balakrishnan, B. (2019). Insider threat mitigation guidance. *The SANS Institute.* Retrieved from https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307

Changing Culture via a Public Health Perspective

Insider Threat Programs are effective at mitigating the insider threat, but they are largely *reactive* rather than *proactive*. Insider threats are made up of three types of perpetrators: malicious, negligent, and accidental.[91] Malicious insiders have a motivating factor compelling them to commit fraud, theft, sabotage, or any other act that goes against an organization's best interests. For this reason, an ITP is often one of the strongest controls for these types of insiders. However, organizations can proactively work to minimize incidents involving negligent and accidental insiders via a culture change.

Researchers from Carnegie Mellon University have taken a novel approach to changing user behavior toward security. While the research is aimed at all industries, its adoption of a public health approach may make it more effective within the healthcare industry. What this model attempts to do is to frame security behavior and behavioral changes the same way the healthcare industry frames exercise, smoking cessation, sobriety, and other public health crises. It highlights that these changes in behavior are unlikely to change in one educational cycle (e.g., a yearly cybersecurity awareness training), rather the healthcare industry must view this as a long-term issue.[92] The root of the problem (i.e., increased incidents involving negligent and accidental insiders) is human behavior, which requires constant feedback and cannot be shaped overnight.

Security culture may also be changed through the combination of executive buy-in and awareness and the inclusion of employees in the security adoption processes. According to Wellforce CISO Taylor Lehmann, while many sources point to people as the problem, he sees them as a solution. Lehmann notes that, "The culture of a hospital is very much about learning and improving. And collaboration is a huge part of medicine." Lehmann suggests that by democratizing the security adoption process by including employees from the beginning, the people involved become "champions of the initiative and feel personal ownership and pride at the work that they did." Lehmann emphasizes that leveraging the power of involving people early and often with executive buy-in can move your agenda forward -- especially if you need to move fast.[93]

Another public health approach to cybersecurity best practices involves information sharing. Similar to how healthcare facilities must report certain communicable diseases to local and state government, cybersecurity threats facing the healthcare industry should also be shared. Industry-specific Information Sharing and Analysis Centers (ISAC), a non-profit community of critical

---

[91] The CERT Insider Threat Team. (2013, August). Unintentional insider threats: a foundational study. *The Software Engineering Institute*. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

[92] Faklaris, Cori. (2019). Reframing Usable Privacy + Security to Design for "Cyber Health." Presentation given to the 2019 Women in Cybersecurity conference, March 29, 2019, Pittsburgh, PA, USA. Retrieved April 4, 2019 from https://www.slideshare.net/CoriFaklaris/reframing-usable-privacy-security-to-design-for-cyber-health

[93] Lehmann, T. (2019, April 23). CMU Interview with Taylor Lehmann [Telephone interview].

infrastructure owners, are an effective resource to gather and provide critical cyber threat information within the private and public sectors.[94] Healthcare industry personnel can report vulnerabilities, threats, and incidents to the Health-ISAC (H-ISAC), which is a vital step to preventing and controlling the spread of cyber and physical threats within the healthcare industry.[95]

Conclusion

In the past century, the healthcare industry has continuously innovated by incorporating new technologies into the field. While they have significantly improved the quality of life for many patients, these innovations have also resulted in expanding the attack surface and exposing healthcare organizations to more risk. These vulnerabilities stem from the potential exploits of incorporating emerging technologies and the increasingly complex processes within healthcare. The healthcare industry not only faces threats from traditional malware such as ransomware that can disrupt hospital services, but also the threats from an insecure supply chain and the devices they depend on. Additionally, emerging technologies further complicate the threat landscape faced by the industry. The implication of national security within healthcare also poses a concern as a breach in the industry can impact millions of Americans. With the current security posture, the healthcare sector will require cost effective solutions to mitigate the new threat landscape. This can be done by leveraging existing frameworks and strategies and by utilizing emerging technologies to detect threats before they impact the organization. By applying a stronger focus in security, the healthcare industry can reap the benefits of innovations while limiting the potential risks they face from cyber threats.

[94] (2019). About ISACs. *National Council of ISACs*. Retrieved from https://www.nationalisacs.org/
[95] (n.d.). About health information and sharing center. *Health-ISAC*. Retrieved from https://h-isac.org/about-h-isac/