University of Houston – College Of Technology

CIS 6326 – Critical Thinking in Info. Sec.

Cyber attacks – An Affliction To Healthcare Industry

Paper Submission

Dhanaraj Chalil

dvchalil@uh.edu

Submitted on: 25th April 2019

TABLE OF CONTENT

Cyber attacks – An Affliction To Healthcare Industry

ABSTRACT

This paper will talk in detail about cybersecurity in the healthcare industry. There were several incidents in the past few years where healthcare data were compromised, hospital systems were hacked, and even cyberterrorism has kept its foot in this industry. So, it is time to think about this arising concern. Research even showed that synthesized DNA which contains gene encoded with malware can be used to hack computer program and systems. So, cybersecurity to the healthcare sector has become a very serious concern, even then healthcare organizations are still lagging in understanding the situation and adopting necessary defense.

This paper will further focus on cyberattack incidents in the healthcare sector, describing those frequent threats that affected healthcare data and machinery. An analysis of the current security posture of the healthcare sector will be presented. An essential thought on the impact of cybercrimes in the healthcare sector and idea on how it will concern the whole world is relevant in this paper. Cyberterrorism has become so threatening issue to different sectors, still, healthcare has its own concern and importance. It is necessary to think about this too as attackers have already turned their focus into healthcare data and genomics. Apart from usual hacking and compromising activities, this section will describe on rapid improvement in DNA sequencing in genomic sciences, and how synthetic DNA can be used to attack computer systems or spread malware, and possible defense against this attack.

The final part of the paper will identify major vulnerabilities that could lead to breaking in of attacks to the healthcare sector, and analysis on guidelines for enhancing cybersecurity to this field. Moreover, it will put light on the importance of security hygiene to the healthcare industry.

1. Introduction

Security threats are a genuine concern for the healthcare sector. There have been several security breaches in healthcare which resulted in billions of dollars of damage and high personal cost for people whose identifiable and private information were unprotected. It is so serious matter to you when your health data being held hostage by hackers. The U.K.’s healthcare industry recently suffered one of the devastating cyber breaches ever. WannaCry, a fast-moving global ransomware attack shut the NHS systems down for many hours. Healthcare establishments all over the country were unable to access patient records or schedule procedures. Appointments were postponed, and operations got canceled while experts worked to resolve the issue.

According to Healthcare Cybersecurity Statistics 2018, a financial loss of $3.62 Million per breach was estimated for organizations which included stolen funds, days spent investigating and repairing, as well as paying any fines or ransoms. It is expected to have increased in cybersecurity threats for the healthcare sector for the coming years. According to the latest trend in the healthcare sector, all personal and patient records are stored digitally, along with payment information, insurance, and transaction details. The digital storage of data, electronic record sharing, and existing vulnerabilities made healthcare a hot target for hackers. Attack on medical centers and organizations can result in long-lasting damage to the institution's reputation too.

Even though technological progress and global interconnectivity was in rapid pace for past few decades brought us numerous benefits, there are disastrous consequences in terms of advanced persistent threats, DDoS attacks, malware infections, cyber espionage, and data and intellectual property theft. Moreover, the healthcare industry is also vulnerable to the damages that occur with the illegal use of personal and confidential information. In fact, about 90 percent of health institutions experienced cyber-attacks since 2012. With cyber-attacks becoming more purposeful, sophisticated, and advanced, the healthcare industry is having to come to terms with its exposure to cyber risks.

The integration of medical devices, networking, software, and operating systems means that the relative isolation and safety of medical equipment, systems, and other important assets of healthcare sector became complex and challenging. The term 'cybersecurity' is used to cover a broad spectrum of context-specific adversarial challenges, which includes the safeguarding of computer networks and information from penetration and malicious damage, the inevitable crossover from standalone medical devices to integrated instrumentation, networks, and software. Regulatory authorities have responsibility for assuring the safety and security of medical equipment. The regulatory bodies have acknowledged the seriousness and enormity of the matter by publishing recommendations for managing cybersecurity risks and for protecting patient health information, to help manufacturers in their submissions for FDA approval of medical devices.

Innovative models of healthcare are facilitated by the opportunity for interoperability while supporting improvements in patient safety. However, the proprietary nature of previously non-interoperable medical devices has limited integration between vendors' products and can result in errors in communication upon integration. Integration does not equate to interoperability, and interoperability does not equate to security. This also brings a serious concern for introducing advanced models to healthcare.

2. Healthcare security, an arising concern to the world

The once seemingly futuristic exploit of implanted medical devices has been made present with the demonstration of successful attacks against devices such as the insulin pump and pacemakers. Research from Ann Arbor Research Center for Medical Device Security at the University of Michigan has demonstrated this potential compromise to implanted devices. This indicates that the lack of device embedded security controls is of greater concern than the incidents they result in. Research has demonstrated that issues such as embedded web services with unauthenticated and unencrypted communication, web interfaces to infusion pumps, default hard-coded administration passwords, access to the Internet through devices connected to internal networks, are some common vulnerabilities found in devices used. Incidents such as a malware attack that infected US Department of Veterans Affairs medical devices running over a trusted network, has led to an isolation approach to protection for some medical devices. Such incidents, together with the national Ponemon and SANS research reports, impelled the US Federal Bureau of Investigation (FBI) to investigate health care as a potential high-profile risk.

The potential for an attack on the healthcare sector by cyber terrorists is very real. Healthcare sector faced ransomware attacks in recent years. As the digitalization of healthcare data continues, the more nefarious activity could follow this change. The cyberattacks on health centers reveal that there are security holes, weak points, and several vulnerabilities that can be exploited by cyber terrorists. Moreover, the assaults on the public infrastructure, most notably water and power supplies, have the potential to cripple the healthcare system. Another likely target is the electronic health record, with which cyber-attacks can be categorized into three categories: the exposure of private or sensitive data, manipulation of data, and loss of system integrity. A disgruntled employee or an insider with a list of active passwords and access to a hospital’s systems have the potential to cause far more damage than outside hacker. Authorized individuals can download sensitive data, drop nasty viruses into the organization’s network, and even open back doors for further exploit. These insider attacks can cause greater damage because they typically are much more targeted and likely to impact the trust level of the people. That could be the aim of many of these cyberterrorist attacks on healthcare. Trust of patients diminishes, and risk ascends if medical or financial data are modified or accessed by unauthorized individuals, manipulated information leads to medical errors, and data are made public without proper consent. Meanwhile, a global study by NetDiligence of cyber insurance claims in 2017 found that healthcare accounted about 18 percent of breaches across all sectors and that 63 percent of these breaches were caused by criminal or malicious activity. There were several high-profile ransomware incidents in the last few years. This represents a new kind of cyber risk, which is well targeted, an orchestrated attack that can have a high impact along the healthcare supply chain.

In May 2017, the WannaCry ransomware outbreak provided an early indicator. This event affected mostly hospitals belonging to the National Health Service (NHS) in the United Kingdom; only a few hospitals were affected elsewhere, including in the United States. SamSam, which struck later in the year, was a different story. While most ransomware typically does not focus on specific organizations and is delivered via generic e-mails, SamSam exploited external-facing vulnerabilities or stolen credentials to penetrate targeted organizations. Several factors shape healthcare's cyber risks:

1. The industry's rapid adoption of digital systems.
2. The emergence of health data as a high-value target for cybercriminals, from sensitive patient data to confidential research and intellectual property.
3. The rise of healthcare organizations as high-profile targets for hacktivists and nation states.
4. The technical and organizational complexity of the industry, which makes it difficult to implement and maintain tight security controls.

3. Key assets and threat landscape of the healthcare industry

A recent research study report on securing hospitals by the Independent Security Evaluators (ISE), identified the primary assets found in the healthcare ecosystem. The most critical one is the patients' health that can be affected in many ways. Patients can be injured through direct actions such as performing inadequate medical acts or turning off critical active medical devices and also by indirect actions aiming at disrupting care. Altering patient health records, compromising medicine inventory systems or cutting off the power supply in operating rooms are likely to have dramatic consequences on the health of the patients involved. The second most important asset in hospitals is patients' health record that contains valuable information including personally identifiable information (PII) such as social security number, health care provider information, credit card information, name, address, date of birth, etc. They also include protected health information (PHI) - like patient physical or mental health condition, provision of health care, etc. that identifies the patient. Nowadays, most of these records are electronic and so exposed to cyber threats. Patients' health records are adversaries' primary target for the purposes of identity theft and other insurance fraud opportunities. Furthermore, attacks on EHRs may have consequences on patients' health when they compromise their integrity whether by altering or destroying sensitive information like blood group, medical history, and so on.

The availability of healthcare services can also be considered as a major asset of medical facilities. They can be divided into two distinct categories: critical services that ensure continuity of care, including, among others, active/passive medical devices, medicine delivery systems, and surgery equipment & administrative services which are dedicated to the smooth hospital workflow. The disruption of critical services may have a devastating impact on patients' health. Systems handling work orders, medicine inventories, prescriptions, bills or appointments are part of administrative services.

Some healthcare facilities host research labs which will contain intellectual property assets such as experimental procedures for surgery, test and studies results, test subject information or drug formulas. This data has high value for the research team, but also for third parties like researchers or pharmaceutical companies of competitor countries. Hence, they can also be identified as targets of cyber-attacks. The alteration of these assets can have even more serious consequences as it may mislead researchers.

The reputation of healthcare facilities and their physicians is also a non-negligible asset. A cyber-attack will harm the institution credibility if it is disclosed to the public. In addition, if the identity of specific medical staff is used to perform the attack, it may damage their reputation and career too. On an average, it could be stated that healthcare facilities have been victims of one cyber-attack per month over the past 12 months and that half of them have experienced the loss or exposure of patient information during this same period. This phenomenon can be explained by the combination of two factors: the high value of healthcare facilities' assets and the ease in which they can be compromised. In fact, the healthcare industry is behind other industries in protecting its infrastructure and its data.

On moving to threat landscape, cyber threats on healthcare facilities can be divided into two categories: the untargeted attacks that do not discriminate between assets, and the targeted attacks which have specific assets in the crosshairs. Adversaries whose target is to maximize their gain/cost ratio, perform the untargeted attack. But for targeted attacks, adversaries have precise objectives and are willing to mobilize the required resources to reach them. The adversaries' motivation is the fundamental difference that exists between the two types of attacks explained. This implies that healthcare facilities cannot defend themselves against targeted and untargeted attacks in the same way. Indeed, while limiting security breaches may be enough to prevent untargeted attacks from happening, a more advanced security policy is required to effectively respond to targeted attacks. The following paragraph gives an overview of the most likely adversaries faced by healthcare facilities as well as their intentions regarding the key assets.

Individuals and small groups of hackers constitute the first category of attackers. They are motivated to financial profit and notoriety. They choose their targets based on opportunity and usually make use of unsophisticated tactics of attack. The second category constitutes political groups and hacktivists. They are motivated by political and financial gain and hacktivism. They often aim at humiliating, discrediting, blackmailing or selling information about high profile individuals. As for criminal organizations, they are motivated by financial gain and more broadly criminal activities such as extortion, blackmail, coercion. They can be identified as the third category of adversaries, mostly aimed at obtaining medical records about target individuals, threatening them or causing harm to them. They may also profit from the exploitation of untargeted EHR in volume. Terrorists, fourth and utmost threatening group, are motivated by inspiring fear and cause harm. Their objective is usually to harm or threatens individuals. Nation-state attackers are also another large aggressive group to be faced, with almost the same motive, which can be included in the fourth category of adversaries.

4. New security threat in genomics – Synthesized gene with malware encoded to hack systems

There has been rapid improvement in sequencing and analyzing approaches of DNA. Modern sequencing techniques can sequence hundreds of millions of DNA strands simultaneously, resulting in a proliferation of new applications in several domains ranging from personalized medicine, ancestry, and even the study of the microorganisms. Lab equipment and computers are needed to process, analyze, and store the billions of DNA bases that can be sequenced from a single DNA sample. Even the sequencing machines themselves run on computers. New and unexpected interactions may be possible at this boundary between electronic and biological systems. Research to analyze new computer security risks that could be possible in the interaction between biomolecular information and computer systems, focused on two key perspectives:

1. The failure of DNA sequencers to follow best practices in computer security – After DNA is sequenced, it is usually processed and analyzed by several computer programs termed as DNA data processing pipeline. An analysis was done on the computer security practices to program this pipeline and it was found that they did not follow computer security best practices, programming languages known to contain security problems were used and identified the presence of vulnerable code. This basic security analysis implies that the security of the sequencing data processing pipeline is weak.

2. The possibility to encode malware in DNA sequences – DNA stores standard nucleotides as letters such as A, C, G, and T. After sequencing, this DNA data is processed and analyzed using processing pipeline. It is well known in computer security that any data used as input into a program may contain code designed to compromise a computer. This led to the thought to produce DNA strands containing malicious computer code that, if sequenced and analyzed, could compromise a computer.

A biological malware was synthesized by scientists at the University of Washington in Seattle, which is recognized as the first DNA based exploit of a computer system. Researchers led by Tadayoshi Kohno and Luis Ceze have incorporated a malware into a genetic molecule, which allowed them to take control of the system that was used to process the genetic data after it was read by a DNA sequencing machine. The researchers warn that hackers could one day use faked blood or spit samples to gain access to university computers, steal information from police forensics labs, or infect genome files shared by scientists.

To make the malware, the team translated a simple computer command into a short stretch of 176 DNA letters, denoted as A, G, C, and T. After collecting copies of the DNA from a vendor, they fed the strands to a sequencing machine, which read off the gene letters, storing them as binary digits, *0*s, and *1*s. Researcher says that the attack took advantage of a spill-over effect when data that exceeds a storage buffer can be interpreted as a computer command. In this case, the command contacted a server controlled by Kohno's team, from which they took control of a computer in their lab they were using to analyze the DNA file.

There is not present cause for alarm about present-day threats. There is no evidence to believe that the security of DNA sequencing or DNA data, in general, is currently under attack. Instead, these results as a first step toward thinking about computer security in the DNA sequencing ecosystem. The DNA sequencing community should proactively address computer security risks before any adversaries' manifest. They should follow secure software best practices when coding bioinformatics software, especially if it is used for commercial or sensitive purposes. Also, it is important to consider threats from all sources, including the DNA strands being sequenced, as a vector for computer attacks. The government is currently involved in regulating the production of synthetic DNA products that may be used to generate dangerous compounds.

5. Cyber attacks in the healthcare industry

The healthcare industry is plagued by numerous cybersecurity issues. These range from malware that compromises the integrity of systems and privacy of patients to distributed denial of service (DDoS) attacks that disrupt facilities' ability to provide patient care. For healthcare, cyber-attacks will have devasting consequences beyond financial loss and breach of privacy. Following details describes a unique attack that the healthcare sector faced frequently.

1. Ransomware – It is hard to ignore the recent increase in reporting of hospitals victimized by ransomware. Ransomware has become such a big concern that the Multi-State Information Sharing and Analysis Center (MS-ISAC), National Health Information Sharing and Analysis Center (NH-ISAC) and Financial Services Information Sharing and Analysis Center (FS-ISAC), teamed up to host training on how to defend against it. Ransomware is a type of malware that infects systems and files, rendering them inaccessible by encrypting the system boot record until a ransom is paid. When this occurs in the healthcare industry, critical processes will become inoperable. This will slow all medical process in

hospitals which will lead to severe medical situations. Typically, ransomware infects victim machines in one of three ways:

- through phishing emails containing a malicious attachment
- via a user clicking on a malicious link hosted in common websites
- by viewing an advertisement containing malware

Recently, multiple hospitals across the United States were infected with ransomware via outdated JBoss server software. In these cases, the attacker uploaded malware to the out-of-date server without any interaction from the victim, as opposed to infecting the hospitals through common workstations used by everyday staff. Actors used an open source tool, JexBoss, to search the Internet for vulnerable JBoss servers, and infected networks, regardless of what industry they were running on. Devices compromised in an infection process are often crucial to a hospitals' mission, and the ransomware may render them inaccessible, delaying patient care while causing tremendous pressure to remediate the issue immediately. This pressure, combined with the fact that hospitals generally have financial resources on hand, potentially increases the likelihood the attackers will be paid.

2. Data Breaches – Data breaches have become another major cyber attack on the healthcare industry. Personal Health Information (PHI) is more valuable on the black market than credit card credentials or regular Personally Identifiable Information (PII). Therefore, there is a higher incentive for cybercriminals to target medical databases and conduct data breaches. PHI is more valuable than PII in the black market because one's personal health history, including ailments, illnesses, surgeries, etc., can't be changed, unlike credit card information or Social Security Numbers. Criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims or to illegally gain access to prescriptions for their own use or resale. The Federal HIPAA Security Rule requires health service providers to protect electronic health records (EHR) using proper physical and electronic safeguards to ensure the safety of health information.

3. DDoS Attacks – Distributed denial of service (DDoS) attacks are a popular tactic, technique, and procedure (TTP) used by hacktivists and cybercriminals to engulf a network to the point of inoperability. While some DDoS attacks are opportunistic or even accidental, many target victims for a social, political, ideological or financial cause related to a situation that angers the cyber threat actors. The DDoS attack case with Boston Children's Hospital in 2014, made the network outage persist for almost a week, with which medical patients and medical personnel could not use their online accounts to check appointments, test results, and other case information. The hospital had to spend more than $300,000 responding to and mitigating the damage from this attack.

4. Insider Threat – The insider poses a severe threat to organizations because the legitimate access they have or had to proprietary systems helps them from penetrating traditional cybersecurity defenses. They also may have knowledge of the network setup and vulnerabilities, or the ability to obtain that knowledge, better than almost anyone on the outside.

5. Business Email Compromise and Fraud Scams – Referred to as the “Billion Dollar Scam” by the Federal Bureau of Investigation (FBI), Business Email Compromise (BEC) scammers use a spoofed email or compromised account to trick employees into initiating a money transfer to a fraudulent account. The scammers almost always pretend to be a person of power within the organization. The scam has been so successful because the actors generally conduct some level of research on their targets first, know how to sound like the individual they are mimicking, and only send the email to a selected people, allowing the e-mail to sidestep basic security strategies such as email filtering. There are multiple variations of this scam, and it affects organizations in every sector and around the world. Hospitals and medical centers need to be wary of this type of scam, which has many variations and could result in lost money, PII/PHI, or goods such as prescription drugs.

Here are key findings from the global study by NetDiligence of 2017 cyber insurance claims:

- Healthcare accounted for 18 percent of breaches across all sectors, tied for the most with professional services.
- Healthcare accounted for 28 percent of breach costs, due to higher than average per-record costs.
- The criminal or malicious activity caused approximately 63 percent of healthcare breaches.
- Hacking was the most common cause of loss in healthcare, with an average breach cost of $2.4 million.
- Ransomware accounted for 10 percent of the costs, with an average cost-per-incident of $76,000.

6. An analysis of the current security posture

The health industry is an attractive target for cybercriminals as health data contains sensitive personal and financial information. To circumvent the breach of healthcare data, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) implemented physical and technical safeguards to ensure sensitive information is protected. Physical safeguards include workstation use and security, device and media controls, and facility access controls. Technical safeguards include a unique user identification number, emergency access procedure, automatic logoff, encryption, and decryption. However, cybercriminals are finding ways to breach these safeguards.

The Privacy Act of 1974 was the first major U.S. legislation to address how personal information is handled by third-party organizations. The healthcare sector is an excellent example of a third-party organization, which by necessity must hold the personal information of others. As the providers of a vital service in the form of medical care, healthcare organizations need to have patients' personal information on hand and readily accessible to provide optimal and effective medical attention. Since this situation creates significant potential for a patients' personal information to become exposed, healthcare organizations must take steps to keep data secure in order to protect the privacy of their patients. Many healthcare institutions are not proactive when it comes to implementing precautionary security measures and putting effective privacy safeguards in place. This has been an ongoing and costly challenge running into the billions of dollars in damages. Proactivity involves cybersecurity strategies to keep pace with cybercriminal attempts to infect systems with malware, steal data such as protected health information and intellectual property as well as to conduct espionage. The federal government has addressed these issues in the form of the Health Insurance Portability and Accountability Act (HIPAA), and subsequently the Health Information Technology for Economic and Clinical Health Act (HITECH).

Different studies on healthcare security posture identified that there is a lack of awareness of healthcare facilities managers regarding the sophistication of hackers and their means to infiltrate confidential patient data networks. It is also identified that there are failures in properly addressing modern security threats at three different levels: organizational, technical and physical.

At the Organizational level, the main issue is the lack of funding dedicated to Information Security. Information Security is not seen as a priority in most facilities. Indeed, in the medical community, protecting patients' health is associated with direct means such as physicians' skills, treatments, medical devices, etc. but rarely with cybersecurity. Thus, the root of the funding problem is the lack of awareness that exists in hospitals, about the critical role of Information Security in ensuring patients' safety. Besides, most of the other cybersecurity-related problems encountered by hospitals stem from the lack of resources they have in this domain. This is illustrated, among others, by the small size of the Information Security staff in healthcare facilities. When the hospital does have an IS staff, an improper organizational structure may prevent them from having enough leverage to define strong security policies. Moreover, security policies were often found defaulting in several hospitals. In some, policies appear to be either not implemented, not enforced or not auditable as their requirements were not precise enough. Finally, hospitals staff (medical or not) receive no or minimal security training.

They show a weak risk awareness and understanding of the threat landscape increasing the hospital vulnerability to cyber attacks.

To the technical level, it is noticed that most hospitals do not have full knowledge of their IT infrastructure. Indeed, few of them have a precise picture of their network, the devices it is made of, etc. and documents to summarizing this information. This inevitably allows security breaches and vulnerabilities to develop as updates and upgrades are delayed, devices misconfigured, and legacy systems kept online although no longer used. Healthcare facilities also have difficulties in understanding, tracking, reporting and managing threats effectively. Mature incident and vulnerability management processes are lacking in most organizations, and thus, daily threats aren't even reported. Most hospitals' networks are designed without considering security matters. Their architecture makes difficult or even impossible for the implementation of efficient security controls. In fact, most hospitals 'networks are little or no segmented and implement poor access controls. Finally, healthcare facilities make extensive use of legacy systems. In fact, numerous hospitals still rely on devices that are no longer supported. They keep using these systems as they are still operational and that upgrading them would be too costly and constraining. Legacy systems vulnerabilities can indefinitely be exploited since patches are no longer released to fix them.

Physical security is not directly linked to the cyber-threats. However, it cannot be neglected as physical access to the hospital network is quite easy in most facilities. Indeed, most patient rooms offer connection to the network as they expose open ports normally used for plugging medical devices. Therefore, attackers can easily create situations allowing them to access these network entry points. It is observed that no security measures are implemented for detecting the connection of intruders to the network, through there open ports. Many systems such as mobile workstations, unattended terminals, medical devices, and wireless access points are within the physical reach of guests. Thus, adversaries could modify or gain control of a device to establish a foothold on the network or harm a patient. Preventing them from physically accessing these devices seems difficult, even unrealistic. Thus, given the current state of cybersecurity in hospitals, protection against cyber threats cannot be strengthened by solely patching systems. In fact, the manner in which security is understood by the healthcare industry must fundamentally change so that effective security can be implemented.

7. Defending cyber-attacks and enhancing security

We have already described on various cyber threats that have stricken the healthcare industry. Following points describes recommendations to defend or mitigate these attacks in the future.

- Ransomware – The MS-ISAC's primer on ransomware outlines the crucial steps every organization should take to heighten defenses against ransomware by properly securing networks, systems, and the end user. Having the incident response, maintaining latest backup of critical data, good patch management, disabling macro scripts, adding of warning banners to emails, restricting internet access, applying the principle of least privilege and network segmentation, increasing security controls, monitoring third-parties, and participating in cybersecurity information sharing are the recommendations mentioned to harden your organization against the threat of ransomware.

- Data Breaches – Proper application security and network security are important to prevent a compromise from happening in the first place. Encryption is the best way to protect patients' data from data breaches and further attacks. It is important that encryption is implemented both at rest and in transit and that third parties and vendors that have access to your healthcare network or databases are also properly handling patient data. Training on proper usage and handling of PHI is recommended to reduce data breaches caused by employee error.

- DDoS Attacks – DDoS attacks occur in a variety of ways and understanding which type of attack is occurring is an important part of being able to properly mitigate the attack. The MS-ISAC guide to DDoS attacks is the best reference for planning defense against the DDoS attacks. General recommendations for defense against DDoS attacks include maintaining an effective partnership with your upstream network service provider as well as partnering with companies that provide DDoS mitigation services.

- Insider Threats – The best way to defend an insider threat is through employee and users training on how to recognize and report an insider threat or prevent them from unintentionally becoming prey for it. There are many open source resources on insider threats with training programs and educational materials for organizations and their employees. Moreover, healthcare facilities should keep track of physical and digital access controls of employees and investigate rapidly whenever unauthorized or unusual access made to network and systems.

- Business email compromise and fraud scams – Increased awareness and understanding of these types of scam is the best way to prevent employees from falling for them. Additional validation steps before performing any crucial activity or transactions to verify legitimacy could help in avoiding scams. Beware of sudden changes in previously standard business practices.

The truth is that healthcare institutions are under a significant threat. Other general recommendations to mitigate cyber-attacks and enhance security in the healthcare sector include the following practices.

- Consider threat entry points – An entry point is a generic term for a vulnerability in your system that can be easily penetrated by hackers. By exploiting this vulnerability, hackers can deploy a virus to slow your network, access critical health information, or remove defenses to make your system more accessible in the future. Malware can be introduced from any vulnerable spot in your network or operating system. Moreover, medical software and web applications used for storing patient data were found to contain numerous vulnerabilities. Patch management should be deployed to cover up all these vulnerabilities.

- Focus on Employee Security training – Cybersecurity professionals employ robust firewalls and other defenses, but the human factor remains a weak link. To minimize human error, system admins need to remind all staff about risky behavior continually. Educate employees on how to recognize legitimate and suspicious emails, threats, and sites so they can avoid phishing attacks. Proper awareness of all kinds of social engineering threats should be provided to employees. Training should be refreshed regularly or customized for different employee groups.

- Healthcare industry cybersecurity should go beyond employee access – Patient concerns about sensitive data security and IT in healthcare should be kept in mind when creating safer, stronger systems, or improving cybersecurity frameworks after a hospital was hacked. System administrators should also make sure that threat intelligence funding remains a priority, which means continuing to invest in security initiatives.

- Consider cloud migration for data – The cloud offers a secure, flexible, and cost-effective solution for healthcare data storage and backup. It also provides a possibility to scale resources on demand, which can bring significant improvements in the way healthcare organizations manage their data. Cloud-based backup and disaster recovery solutions ensure that patient records remain available even in case of a breach or downtime. Combined with the option to control access to data, these solutions can provide the needed level of security.

- Ensure vendors Are Compliant – The vendors should take proper steps to monitor and detect threats, as well as to limit access to their systems. Insurance companies, infrastructure providers, and any other healthcare business partners must have spotless security records to be able to protect medical information. This is especially important for organizations that outsource IT personnel from third-party vendors.

- Ensuring HIPAA Compliance – Larger healthcare organizations have at least one person dedicated to ensuring HIPAA compliance. Their primary role is creating and enforcing security protocols, as well as developing a comprehensive privacy policy that follows HIPAA recommendations. Educating employees on HIPAA regulations can contribute to creating a security culture. It also helps to assemble specific HIPAA teams, who can also share suggestions on how to restrict healthcare data or further cyber defenses in the organization.

- Push a top-down Security Program – Every medical facility likely has a security staff and an IT team, but they rarely overlap. Adding healthcare cybersecurity duties at a managerial level, even as an executive position, can bring multiple benefits. It can make sure correct initiatives are created, launched, and enforced, as well as that funding for security initiatives is available. With cyber security threats, being proactive is the key to ensuring safety long term. Regular risk assessments should be part of any healthcare provider's threat management program.

- Hospitals can consider engaging in regional or national information-sharing organizations to learn more about the cybersecurity risks faced by hospitals, employees as well as senior managers should be aware of all the risks they face when using their IT and learn how to reduce these risks with a compliant use.

8. Security hygiene for the healthcare industry

The devasting impact of the Petya and WannaCry ransomware attacks were a direct result of businesses failing to have the basics of cyber hygiene. Many organizations and employees are still unaware of the importance of security hygiene in defending cyber attacks. They do consider only technical solutions to make a secure environment. Inadequate cyber hygiene has been building risks over a long period of time. Enterprises find it incredibly difficult to demonstrate active control over their cyber hygiene and thus efficiently remediate top cybersecurity risks. This is because the larger the organization, the more challenging it is to maintain these 'basics,' of security hygiene. In the hospital setting, there is no tolerance for poor cleanliness. It's just as important to commit to security hygiene to slow down attackers who are looking to infect healthcare industry. Following are some recommendations to implement security hygiene in the healthcare industry.

1. Encryption – Encrypting wherever feasible is the best way to secure your data. This offers less risk even if the health records or assets maintaining it breaches since data stays encrypted and does not get exposed. Offering a backup option will help in restoring data and operations after a breach.

2. Prioritize rigorous patching and patch management – The vendors create patches for their products to defend against new vulnerabilities. Deploying patches can be a bear of a process, but it needs to be a high priority for organizations. This will help to stay safe in today's threat landscape.

3. Replace unsupported legacy software or hardware – Replacing unsupported legacy software and other products will require capital expenditures, but it's very necessary to protect data and ensure business continuity. Legacy systems will have a lot of vulnerabilities that are easy for attackers to exploit and attack. This event provides an option for attackers to keep a foothold on the organization network for performing advanced persistent threat.

4. Limit users who have local administrative rights or controlling access – This can be a challenging process. But, this is an imperative step to limit lateral movement if malicious hackers get into your network or networks, and to reduce the threat of malware attacks.

5. Implement multi-factor authentication – This should be considered for limiting administrative rights and remote access to systems that house sensitive information or PHI. Defense in depth strategy is vital to protect healthcare data and assets.

6. Sandbox for advanced protection – It is important to keep up with more advanced technologies and techniques to deal with constantly evolving threats. Sandboxes, or automated malware analysis appliances, can be deployed either inside or outside of the network to test files in a virtual environment to determine if they are malicious.

7. Perform security log collection, monitoring, and analysis – This is a vital step to analyze, detect, and respond to any malware or intruder attacks. It even serves as an input for figuring indications of compromise in the network. A security team hosted in the healthcare facility or an outsourced Security Operation Center can handle this task effectively.

8. Commit to incident response planning and preparedness – An effective incident response is a process that requires ongoing commitment and ongoing management. It is an organized approach to address and manage the aftermath of a security breach or cyber attack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

9. Increase the need for network segmentation to isolate exposed devices – It is important to isolate your exposed devices to limit the impact of an attack away from your most critical data. This could even help in blocking the lateral movement of malware that tries to spread its infection.

9. Conclusion

Many healthcare facilities are still poorly equipped with strong security measures. However, being proactive and aware of ever-changing security risks can help in implementing a strong defense against cyber threats. We have seen the importance of having cybersecurity in the healthcare industry, but the organizations should start considering it to be one of the important factors for securing patient health and data. Having a dedicated security team or outsourcing it for good services, educating employees, enhancing vulnerability and risk management, and compliance with regulations will help healthcare infrastructures battle against cyber attacks. It is advised to start a threat management program today itself.

Patient safety will always come before cybersecurity requirements. The challenge lies in closing the gap between objectives of minimizing compromise to ensure patient safety and being responsive to the cyberattacks. Medical devices are an integral component of medical networks and their security should be an integral component of cybersecurity protection. This needs an excellent collaboration between the medical physicists and IT professionals, as well as a collaboration by medical device manufacturers and network vendors, and require input from cybersecurity experts.

The cybersecurity vulnerabilities that are associated with medical devices are similar to any other networked system. The difference lies in the potential detrimental impact on patient safety that the exploitation of vulnerabilities may have. To shift the protection of medical devices to more mainstream cybersecurity protection will require the acceptance of medical devices as standard connections in the network. To ensure the future protection of medical devices in a networked world, a coordinated proactive approach that includes standard cybersecurity assessment and control, together with specific medical device data and workflow considerations, is needed.

A list of cyberattacks that targeted healthcare in past years put forward a sharp reminder that the healthcare industry is still at risk, and organizations have not adopted proper measures to offend and defend it. For the current threat situation and security posture of organizations, it's predicted that these types of attack will become advanced, broader, and frequent. The knowledge and technology gaps between device manufacturer, other vendors and medical cybersecurity firms should be filled.

REFERENCES

1. *Cybersecurity in healthcare: A systematic review of modern threats and trends – https://content.iospress.com/articles/technology-and-health-care/thc1263*
2. *U.S. Department of Health and Human Services. Fact sheet: ransomware and HIPAA - http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf*
3. *Is cybersecurity possible in healthcare? – http://publications.excelsior.edu/publications/NCI_Journal/index.html*
4. *Healthcare Information – A new terrorist target – https://www.fortherecordmag.com/archives/0413p10.shtml*
5. *Cybersecurity in Hospitals: A Systematic, Organizational Perspective – Monitoring Editor: Eric Perakslis, Reviewed by Mark Jarrett and Navid Ghaffarzadegan, Mohammad S Jalali, MSc, PhDcorresponding author1 and Jessica P Kaiser, MBA – https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/*
6. *Cyber Security Threats to Public Health – Daniel J. Barnett, Tara Kirk Sell, Robert K. Lord, Curtis J. Jenkins, James W. Terbush, and Thomas A. Burke – http://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2013/Cyber%20Security.pdf*
7. *State of cybersecurity & cyber threats in healthcare organizations: Applied Cybersecurity Strategy for Managers – Aurore LE BRIS, Walid EL ASRI – https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf*
8. *Cyberterrorists targeting healthcare systems, critical infrastructure – https://www.abc.net.au/news/2017-10-23/forget-explosives,-terrorists-are-coming-after-cyber-systems/9076786*
9. *Defending hospitals against life-threatening cyber attacks – https://www.scientificamerican.com/article/defending-hospitals-against-life-threatening-cyber-attacks/*
10. *Healthcare cybersecurity predictions for 2019 – https://www.cybermdx.com/blog/healthcare-cybersecurity-predictions-for-2019*
11. *HIPAA Journal – https://www.hipaajournal.com/category/healthcare-cybersecurity/*
12. *Reasons why hackers are targeting healthcare providers – https://www.assurancesoftware.com/product-blog/reasons-cyber-hackers-are-targeting-healthcare-providers*

13. *Hacking healthcare IT in 2016 – Institute of critical infrastructure technology – https://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf*
14. *Exploring the cyber threats to healthcare – https://www.secalliance.com/blog/exploring-the-cyber-threats-to-healthcare/*
15. *How Ransomware Affects Hospital Data Security – https://healthitsecurity.com/features/how-ransomware-affects-hospital-data-security*
16. *Healthcare must move from risk to resilience – https://www.healthcareitnews.com/news/healthcare-must-move-risk-resilience*
17. *Security and Privacy After September 11: The Healthcare Example: Peter.P.Swire & Lauren.B.Steinfeld – https://heinonline.org/HOL/LandingPage?handle=hein.journals/mnlr86&div=43&id=&page=&t=1556171843*
18. *Multi-State Information Sharing and Analysis Center – https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf*
19. *MS-ISAC Security Primer Ransomware – https://www.cisecurity.org/white-papers/ms-isac-security-primer-ransomware/*
20. *Center for Internet Security Nationwide cybersecurity review – https://www.cisecurity.org/white-papers/ms-isac-security-primer-ransomware/*
21. *Why Data Security is The Biggest Concern of Health Care – https://healthinformatics.uic.edu/blog/why-data-security-is-the-biggest-concern-of-health-care/*
22. *Healthcare cybersecurity: Tips for securing private health data – https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data*
23. *Data security in healthcare – https://www.youtube.com/watch?v=pplgLvEE8aw*
24. *Proactively protect against healthcare data breaches – https://www.databreachtoday.com/proactively-protect-against-healthcare-data-breaches-a-9027*
25. *The anatomy of healthcare data breach – https://www.cleardata.com/webinar/anatomy-healthcare-data-breach/*
26. *Biohackers encoded malware in a strand of DNA – https://www.wired.com/story/malware-dna-hack/*
27. *UW DNA Sequencing Security Study – https://dnasec.cs.washington.edu/*
28. *Researchers encode malware in DNA, compromise DNA sequencing software – https://arstechnica.com/science/2017/08/researchers-encode-malware-in-dna-compromise-dna-sequencing-software/*
29. *SANS Security Awareness: Malware encountered involves attacking the human – https://www.sans.org/security-awareness-training/blog/97-malware-encountered-involves-attacking-human*