International Journal of
Technology and
Systems
(IJTS)

Cyber Security as a Threat to Health Care

Cyber Security as a Threat to Health Care

Adegoke Adebukola, Achen Navya, Foreman Jordan, Nwaobi Jenifer, Richard D. Begley

Marshall University Department of Computer Science and Engineering Building

Corresponding Author’s Email: adegoke@marshall.edu

ABSTRACT

Purpose: Cyber security incidents are posing an increasing risk to the healthcare industry. The healthcare industry has lagged behind other industries in protecting its most important stakeholder (patients), and hospitals must now invest significant capital and effort in protecting their systems**.** The goal of this research was to understand the complexities of the operating environment as well as document the technological vulnerabilities to avoid cybersecurity incidents. The eight Aggregated Response Strategies (EARS) framework contains 8 methodologies, which could be used by all the personnel in medical services associations. The secondary hypothesis derived out of this research was the six-step plans introduced by the American Health Association, which aided in ensuring cybersecurity with facilities and organizations in cases of potential threat.

Methodology: The methodology used to derive this hypothesis was through literary reviews, which constituted research articles, journals, and peer-reviewed articles published between 2005 and 2021. These were obtained from PubMed, Google scholar, NCBI, ScienceDirect, CDC.gov, CMS.gov, and Census.gov databases.

Finding: The finding suggested overall security awareness and training must be established immediately after a potential threat is detected. Authorities advise against paying ransomware attackers since there is no assurance that an attack will be reversed, Law enforcement should be immediately contacted in the event of a ransomware attack besides cloud data backups will make it simple to rebuild networks, disaster recovery planning should be done before a cybersecurity threat occurs.

Keywords: *Cybersecurity, healthcare, health technology, data.*

CYBERSECURITY IN HEALTHCARE

1. Introduction:

1.1 Effects of Cybersecurity

Healthcare apps and medical data are much more sensitive and complex to protect than many other types of data and applications because they need a high degree of protection. Numerous threats may confront healthcare applications, each with its own set of causes and solutions. This paper highlights a few of these security risks (Alharam & El-Madany, 2017).

Disruptive assaults, identity theft, the loss of past medical records, and access to regulated information from laboratories are all examples of security risks.

a) Disruptive Attacks: Shutting down healthcare systems, vital equipment, lab equipment, resetting configuration settings of medical devices (e.g., insulin infusion pumps), or rebooting life-sustaining devices are all examples of disruptive attacks.
b) Identity Theft: This includes impersonating and stealing patient information, as well as insurance fraud.
c) Laboratory access to controlled substances: While the convergence of medical facilities with information and communication technology represents a significant evolutionary step in bringing the medical field to the next level, the protection of these technologies can be seriously compromised by the physical equipment of the health network, and vice versa (Dogaru & Dumitrache, 2017).

There is a variety of medical devices that can be tampered with and modify the setting parameters or to capture data as follows:

a) Therapeutic devices such as opioid or chemotherapy infusion pumps - Changing the dosage of the pumps administered to patients may be life-threatening.
b) Diagnostic equipment - Like the data from PET scanners, X-ray or CT scanners, and MRI machines are stored in a picture archive and communications systems (PACS). Researchers from TrapX Security discovered a malware called MEDJACK that penetrated medical devices like X-ray machines running Windows NT4.0 or MRI machines to gain access to the hospital's PACS, which is extremely big on the black market.
c) Surgical machines or Telesurgery - Through the Interoperable Telesurgery Protocol (ITP), a surgeon may perform remote surgery on a patient using a robot running on a single PC that interacts with a control console with haptic feedback and video ITP. Due to the geographical distance, contact is built over public networks, rendering it vulnerable to security vulnerabilities; an attack vector can change the set point of the surgical robot to make an incision from 1 cm to 1.95 cm, or it can postpone the transmission of command when bleeding must be stopped, and immediate action is taken.

d) Life support equipment - Implantable cardiac devices, such as pacemakers, are used to treat patients with heart failure or irregular heartbeats. Some of these devices use radiofrequency signals for transmission and to receive the data about the patient's heart on a monitoring device, connected wirelessly, which is then sent to the clinician. An embedded computer in this implantable system may be used as a mode of cyber-intrusion to modify the pacing, assess electrical shocks, or even deplete the device's battery.

Most of the issue devices that were vulnerable to cyber-attacks were replaced with newer devices that had software upgrades, but this is not a remedy for reducing the possibility of a security breach (Dogaru & Dumitrache 2017).

1.2 Purpose of Cybersecurity

Electronic healthcare technology is widely used around the world, and it has enormous potential to enhance clinical outcomes and change the way care is delivered. However, the security of healthcare data and computers is becoming a growing concern. Medical devices have been exposed to new cybersecurity vulnerabilities as their access to existing computer networks has increased. Healthcare is an appealing target for cybercriminals for two main reasons: it has a lot of useful data and its defenses are poor. Stealing patient records and malware attacks on hospitals are examples of cybersecurity breaches, as are attacks on embedded medical equipment. Patient faith can be eroded, health services can be crippled, and human life can be jeopardized because of breaches. Finally, while cybersecurity is vital to patient safety, historically, it has a poor track record. To foster reform, new laws and regulations have been enacted. This necessitates the integration of cybersecurity through patient safety. As part of a holistic approach, changes in human behavior, technology, and processes are needed (Coventry & Branley, 2018).

1.3 Review of trends

Cyber-attacks may occur at any network link and any endpoint, according to emerging cybersecurity trends. Interoperability of applications, operating platforms, medical device interfaces, and information sharing networks is critical to cybersecurity risk management in a digitalized health system. Medical cyber-physical streams, wireless networking, and the introduction of medical applications in healthcare have all expanded attack surfaces and vectors exponentially. It is now difficult to secure any point of entry into the healthcare system.

a) Medical cyber-physical systems: This encompasses the Medical Internet of Things (MIoT) both implantable and wearable medical devices. Medical Cyber-Physical Systems (MCPS) are becoming more widely used in hospitals to provide high-quality care, and they have emerged as promising tools for tracking and managing various aspects of patient health. By 2020, it is anticipated that there will be 20 billion connected devices, with 50 billion by 2028. The inherent security threats of MCPS are increased by their inherent features. These characteristics make MCPS diverse, mobile, heterogeneous, and increasingly prevalent. They are often left unattended (as in implantable devices) to record intimate physiological data and are restricted in their size, strength, and memory function which facilitates only basic security capabilities. Because of their proximity and dependence on the healthcare network, MCPS features make them vulnerable to compromise, posing a major cybersecurity risk to the entire healthcare system. MCPS has become a significant potential attack vector for malicious actors to gain access, install malware, and alter care delivery. Cybersecurity measures such as vulnerability scans and patch management are often unavailable or limited to manufacturers. There is a lack of clarification on post-sale ownership, software updates, and MCPS security regulation on a global scale. Since this is considered confidential information, manufacturers may be hesitant to provide documenting system detailing cybersecurity vulnerabilities or patching and upgrade policies. In the absence of healthcare standards to facilitate MCPS interoperability, incompatibility between various healthcare systems and medical devices grows, and a healthcare vendor sector emerges that rushes patient devices to market before cybersecurity concerns are addressed. The Australian Therapeutic Goods Administration has identified the cybersecurity vulnerability of medical devices, as well as the lack of manufacturer and regulatory oversight, as a strategic priority.

b) Data confidentiality, privacy, and consent: The next sub-theme found was the privacy of sensitive patient data and concerns surrounding the use of personal details. Cybersecurity risks to healthcare confidentiality, accessibility, and honesty may be classified as a risk to personal information. Loss of personal health records or data, as well as consumer trust, threaten confidentiality. Denial of service (DoS) malware or ransomware attacks obstruct access to health records, software platforms, operating systems, and hardware. If health data is lost, destroyed, or changed, or if wireless access to vital devices or monitors is disrupted, the health data's integrity is jeopardized.

Due to its economic size and large attack surface, healthcare is both a vulnerable and appealing option for cyberattacks. Given the importance of the health sector and the type of user information contained within health information systems, the health sector should place a greater emphasis on cybersecurity. For patients, service providers, and identity hackers alike, health records and medical data are extremely valuable commodities. Health data is estimated to be ten to twenty times more valuable than credit card or banking information because if the credit card or banking information is compromised, that can be changed. But health records or data that can be traced back to a single person cannot be altered.

c) Cloud computing: Cloud computing has been described as a threat to data and information security during both transmission and storage. Because of the massive amount of health data generated, centralized data storage, encryption, deployment, and maintenance have become prohibitively expensive at the individual organization level. With the introduction of cloud computing, data collection, retrieval, and analysis could be delegated to a remote server. Because of the scalability and reliability of cloud computing, any possible compromise exposes data to a much larger audience. With cloud storage, there are two attack vectors: attacks on data at rest, which modify or substitute information, and attacks on data in motion, which occur during data transfer to or from geographically dispersed cloud servers. To ensure the protection of patient health information and data stored on cloud platforms, encryption technology is required. Attackers could gain access to hypervisor processes and resources (such as a virtual machine monitor, computer software, firmware, or hardware that generates and operates virtual machines) and, potentially, any client application if the host operating system is compromised.

d) Health application (‘app’) security: Health apps' widespread usage and lack of security features have been identified as a growing cybersecurity risk to personal data confidentiality and the integrity of interconnected HCS infrastructure. Huge amounts of recognizable health data can be produced, stored, and processed by health apps. WhatsApp is appealing for telemedicine services in resource-constrained settings and to promote specialist networks and team collaboration because of its ubiquity, flexibility, low cost, and enhanced encryption. Clinicians' use of WhatsApp has become so widespread that urgent guidelines are needed to ensure that clinicians do not unwittingly compromise patient privacy or confidentiality.

Health programs encourage mental health applications as a safe, open, and cost-effective alternative to face-to-face therapy. However, there is little study on the safety and protection of smartphones in medical practice, as well as the proliferation of apps for mental wellbeing and dementia. According to a recent Australian survey, more than half of government-endorsed applications lack a privacy policy that explains how personal information is obtained, stored, and exchanged with others. App developers, who are essentially unregulated in terms of material, authorship, and trustworthiness, often overlook patient confidentiality and protection, as well as the security of communications. A lack of knowledge (n = 106), about the confidentiality or protection of the data collected from their wearable device apps, including what was accessed and how it was transmitted or stored, was found by the author of a cross-sectional survey examining the privacy and information security of health apps in wearable devices. These findings, according to the author, represent a broader lack of awareness about potential data protection and privacy threats among the general public. It's concerning that these applications have gained regulatory approval for use in people with dementia and mental illness. Health applications may be vulnerable to both active and passive attacks, resulting in data modification or theft, if appropriate security measures are not in place.

e) Insider threat: The final sub-theme found (n = 7) was that healthcare cybersecurity mechanisms do not adequately resolve the problem of insider threat as the "entry point" for ransomware. Insider collaboration is involved in the majority of data breaches, whether it is deliberate or not. With email being the most popular vector by which healthcare organizations are targeted, failing to recognize or react to phishing emails remains a significant issue. The majority of insider problems are caused by negligence rather than malice, but an unintentional mistake may be just as harmful, making a lack of health information technology and cyber-hygiene awareness a significant danger. According to studies, respondents use poor or unreliable passwords and are unaware of the protocol for data protection violations. Malicious intent in cyber-attacks is poorly understood, and to fully understand and define its effect on mitigation strategies, human factors must be integrated into cybersecurity risk assessments. Owing to the many threats associated with collaborative sharing in complex healthcare network networks, inadvertent information leaks will tend to persist (Offner, Sitnikova, Joiner & MacIntyre, 2020).

1.4 Threats

385 breaches affecting more than 19 million patient records have been identified by healthcare institutions, with 59 percent including business partners such as manufacturers, suppliers, and contractors. The number of breaches is on the rise due to a variety of factors. Lack of information security awareness training programs for non-IT staff, lack of access control for server rooms, lack of password protocols, lack of data backup systems, and meager IT/InfoSec budgets are among the most common risk factors found by healthcare institutions that have been victims of data breaches. Unauthorized access and disclosure are also common in the healthcare industry. Patients and employees can suffer severe consequences as a result of these possible motivations. In 2014 researchers developed encryption and other tools to reduce the incidence of these events. Unfortunately, another study found that these methods do not minimize the total number of instances of lost published data. As a result, an EHR implementation approach must be adopted that allows the user to face these obstacles during the implementation process (Bouazzaoui & Daniels, 2020).

2. Objective:

2.1 Stating the problem

Medical devices have become more susceptible to cybersecurity vulnerabilities because of increased access to established computer networks. It is important to understand the complexities of the operating environment as well as document the technological vulnerabilities to avoid cybersecurity incidents.

Recent technological advancements have resulted in healthcare delivery transformations that have the potential to enhance patient care. The increased interconnectivity between medical devices and other clinical structures is a prime example of this. Medical devices, like other networked computing systems, are subject to security breaches because of their interconnectivity. However, unlike other networked computing systems, there is growing concern that these medical devices' networking would have a direct impact on clinical care and patient safety. The relative isolation and protection of medical devices were threatened by the convergence of medical devices, networking, applications, and operating systems Complexity and complexities in management, as well as security, accompany integration. The term "cybersecurity vulnerabilities" refers to both issues (Williams & Woodward, 2015).

2.2 Proposing a solution

Despite these risks, as well as the additional dangers posed by cybercrime incidents to patients' safety, as well as organizational and financial challenges to healthcare organizations, few studies have examined cybersecurity threats in healthcare. This study examines the major types of cybersecurity threats for healthcare organizations and discusses the positions of the four major players in cybersecurity (cyber attackers, cyber defenders, developers, and end-users) to help healthcare organizations and policymakers better understand the significance of the problem. Finally, the paper offers policymakers and healthcare organizations a collection of guidelines for strengthening cybersecurity in their organizations. (Bhuyan, Kabir & Escareno, 2020)

3. Summary

3.1 Identification and Management of the problem

The increased integration of technology into the health field is leading to greater precision in healthcare; however, advancements in cybersecurity measures are still required. According to a 2016 report by IBM and the Ponemon Institute, the frequency of data breaches in the healthcare industry has been steadily increasing since 2010, and it is now among the sectors most targeted by cyber attacks globally (Argaw et al., 2020).

Recently, it was reported that over 110 million patients in the US had their data compromised in 2015 alone. Of the 223 organizations surveyed in 2016, only half of these providers think that they are capable of defending themselves from cyber attacks making the healthcare sector an attractive choice for cyber-attackers (Martin, Martin, Hankin, Darzi, & Kinross, 2017). Cyber-attackers chose to focus on the healthcare sector for a couple of reasons: it is a rich source of valuable data, and U.S. healthcare organizations lack a deliberate, organized, and comprehensive cybersecurity framework that promotes cyber-resiliency, which is the ability of an organization to withstand an impact, continue operations and return to the original condition (Chon, Dave, & Ronald, 2019). Although there has been an increase in security governance frameworks with overlapping goals and recommendations, the healthcare industry is found to implement frameworks and tools that are not risk-based.

3.2 Major players in Cybersecurity

Besides the lack of a standard cybersecurity framework and best implementation practices within the healthcare organization, there also seems to be a disconnect between healthcare administration and their organizations' cybersecurity architecture. For cybersecurity governance to be truly effective, top management needs to take a more active approach to learn more about the organization’s vulnerability points, defense safeguards, and key players within the cybersecurity space. Due to the host of individuals and organizations that play a major role in cybersecurity, a list of key players along with the roles they play is listed below. A deeper understanding of their roles in achieving cybersecurity and a recognition of their limitations will aid healthcare organizations in better planning to prevent cyber threats and future breaches.

2.2.1 Cyber-attackers

Cyber-attackers are the most prominent threat to cybersecurity within business information technology infrastructure and are the main focal point when establishing a solid IT security framework. Understanding the motivation of the various type of cyber-attackers can serve as a foundation for building strong cybersecurity protocols. On a micro-level, a hacker is an individual that seeks to gain remote access to data with or without authorization. There are two subcategories of hacking that are differentiated by the attacker's intent and authorization, and therefore can help to identify the type of cyber-attacker and procedures that a cybersecurity team must implement. Attackers use one or a combination of cyber attack methods to achieve their goals (Bhuyan et al., 2020).

2.2.2 End Users

End users also play a critical role within the cybersecurity schema. End-users can either be malicious or non-malicious players, and both can present a specific kind of threat. End users have been acknowledged as being a "weak" link when it comes to protecting organizations against cyber-attacks and establishing an effective cybersecurity framework within a business enterprise architecture. It has been estimated that around 48% of data breaches were linked to company insiders who were either current or former employees, and around 10% of these incidents were unintentional (Bhuyan et al., 2020). Business insiders demonstrating malicious intent are deemed extremely dangerous since they are familiar with the strengths and weakness of the system, however, non-malicious end users may also serve as a gateway for potential cyberattacks (Camp, 2011). A healthcare organization that plans to implement effective security protocols, but fails to prepare its workforce, can be susceptible to cyber-attacks.

2.2.3 Cyber Defenders

The cyber defender is being used here as a broad term that can incorporate a vast array of individuals that are actively working to ensure cybersecurity. The cyber defenders include IT professionals, such as cybersecurity experts, and government agencies. Their primary role is in planning and executing security measures to ensure that their organization is protected from cyber threats. The healthcare field is currently facing a shortage of cybersecurity experts. This shortage can be attributed to low pay and poor recruiting efforts from healthcare organizations (Bhuyan et al., 2020).

2.2.4 Developers

Software Developers are essential to ensuring cybersecurity as it is their application systems and development shortcomings that cyber attackers exploit to breach systems. Malware can easily be introduced into a network when there are oversights made within the programming process by developers. An estimated 90% of security incidents happen through exploiting a vulnerability in a software program, which can be ubiquitous and increasing in number (Chon et al., 2019). While several organizations choose to invest money in protecting their networks, many of these breaches target the application layer. The apparent disconnect between developers and defenders also strains defenders and ultimately weakens cybersecurity. Healthcare organizations need to be aware of this disconnect and try to remove the information silo that exists between developers and defenders (Bhuyan et al., 2020).

2.2.5 Policymakers

In dealing with cybersecurity, policymakers face a constantly evolving target. Furthermore, the regulatory process takes time and can be difficult to change. Because of this, policymakers will likely need to be constantly familiarizing themselves with currents IT trends and educating themselves on best practices revolving around newly adopted technologies as they try to develop cybersecurity policies. As innovations occur, policymakers may need to alter the regulatory environment to allow technological innovations to be applied to healthcare (Bhuyan et al., 2020).

2.2.6 Healthcare Organizations

For healthcare organizations, cybersecurity involves trade-offs. Healthcare organizations also need to be financially prepared for the significant resources needed for successful cybersecurity measures and key IT staff implementation. Healthcare organizations' concern for deciding HIT risk trade-offs seems to present a current trend of "hiding in the bell curve." This involves the idea that an organization does not want to trail its competition in meeting regulations, but there is little incentive to incur the higher cost of outpacing its peers (Bhuyan et al., 2020). Healthcare organizations, like all other organizations, need to take a comprehensive approach to cybersecurity rather than an ad hoc approach of dealing with threats as they appear (Marianna, Mariangela, & Angelo, 2018).

3. Methodology

The primary hypothesis derived from this research was that the development of a response plan acts both as a key coping mechanism and as a defense system against cybersecurity. Eight Aggregated Response Strategies (EARS) framework contains 8 methodologies, which could be used by all the personnel in medical services associations. The secondary hypothesis derived out of this research was the six-step plans introduced by the American Health Association, which aided in ensuring cybersecurity with facilities and organizations in cases of potential threat.

The methodology used to derive this hypothesis was through literary reviews, which constituted of research articles, journals, and peer-reviewed articles published between 2005 and 2021. These were obtained from PubMed, Google scholar, NCBI, ScienceDirect, CDC.gov, CMS.gov, and Census.gov databases. The usage of the internet and Google search engine was restricted to gather more information from government and other private websites. Keywords used for the search were 'Cybersecurity' OR 'Cybersecurity in healthcare' AND 'Vulnerabilities' OR 'Cyberthreats' AND 'Countermeasures in Cybersecurity' AND 'Identity Management and Continuity of operations in healthcare' OR 'Risks, Guidelines' AND 'solutions for Cyber threats'. The inclusion criteria were articles obtained in English and studies conducted across the globe, between 2005 and 2021. A total of 51 literary reviews passed this inclusion and were included in the research. The exclusion criteria were the publication year as the articles used to derive this hypothesis were sourced from 2000 to 2021 and did not include publications from the earlier years to include more relativity to the research paper. This research was done by NA, AA, JF, and JN and validated by BR who enacted the role of a reviewer and assessed if the references met the inclusion criteria.

4. Cybersecurity Characterization

4.1 Cybersecurity Vulnerabilities and Cyberthreats

Vulnerabilities can be defined as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (Marianna et al., 2018). Protecting against malicious software requires not only technical solutions to prevent, detect, and remove the threats but also policies and procedures for reporting suspected attacks. Discussed below are some of the major types of cyber attacks and the motivations behind them so an organization can better understand how these attacks can occur and their impact within a system.

4.1.1 Denial-of-Service (DoS)

Denial-of-service is a cyber attack that aims to flood a network with traffic to disrupt service and prevent users from accessing network resources. This form of attack has the capability of significantly slowing or shutting down the entire network of a healthcare organization. In addition to the financial losses related to restoring systems after a DoS attack, it is particularly dangerous as it can prevent healthcare providers from accessing or transmitting vital information during the attack (Chon et al., 2019).

4.1.2 Privilege escalation

Privilege escalation attacks are driven by the goal of achieving a higher level of access to a network or program. They are typically executed by exploiting vulnerabilities in a program
or network. Cyber attackers could choose to use elevated access to do several things to the system, such as changing a patient's health information, which could compromise the safety and health outcome of the patient (Bhuyan et al., 2020).

4.1.3 Man in the Middle (MITM) or Eavesdropping

An eavesdropping attack occurs when an intruder intercepts communication between two parties. The attacker eavesdrops on the contents communicated by acting as an intermediary in the information exchange. The integrity of the data being communicated can easily be compromised since the intruder can alter the data before relaying it to the other party or parties (Bhuyan et al., 2020). In healthcare, an eavesdropper could gain access to confidential information which can be leveraged by attackers against healthcare organizations for malicious purposes (Gade & Reddy, 2014).

4.1.4 Cryptographic Attack

A cryptographic attack is carried out to reveal information that has been concealed. Cryptography is the process of encrypting and decrypting information into codes, so only the sender and intended receiver can understand it. The binary coding helps to obscure data and information to others because the algorithms used in encrypting the information are only accessible to its creator. A cryptographic attack seeks to decrypt this encrypted information and make it available to the attacker (Bhuyan et al., 2020).

4.1.5 Structured Query Language Injection Exploit

Several websites use the programming language Structured Query Language (SQL) to manage their databases. Vulnerabilities in SQL may be exploited by hackers to execute malicious attacks, or harmful SQL statements, that allow for the data servers to divulge private health information. During such an SQL injection attack, hackers can alter the information in the database, affecting the integrity, confidentiality, and availability of information stored on that database (Bhuyan et al., 2020).

4.1.6 Malicious Software

Malicious software, or malware, refers to a group of programs that are designed to harm or compromise a computer system without the permission of the user. These programs carry out various functions that include altering, damaging, spying, or deleting user information. Malware is spread either physically using an external drive or through internet downloads such as infected emails. Some common malware are worms, bots, viruses, adware, Trojans, spyware, adware, backdoors, ransom ware, and rootkits (Bhuyan et al., 2020).

4.1.7 Phishing

Phishing is utilized through social engineering to trick individuals or organizations, into either divulging information or performing an activity harmful to their computer, gaining unauthorized access to the system network. Phishing could be considered more of a technique, or vector, than a specified type of attack, and is one of the most common ways to deliver malware. Attackers can utilize emails that can redirect the receiver to a website, which either collects their information or prompts the download of malicious software (Bowman, 2013).

4.2 Countermeasures (7-layer “trust” framework)

Managing cybersecurity risk is a balancing act between security and resilience. An organization can rarely ever be completely secure but can develop the capability to recover quickly from a cyber attack. The trust framework outlined below offers seven layers of protection essential for building an effective level of resiliency and can help in establishing and maintaining trust within a healthcare enterprise.

4.2.1 First Layer: Risk Management

Risk is simply the probability that some “bad thing” will happen, and always concerning a given context comprising relevant threats, vulnerabilities, and valued assets. Vulnerabilities are present in facilities, hardware, software, communication systems, business processes, workforces, and electronic data (Saba & McCormick, 2015). The appropriate number of resources and time should be focused on risk assessment to appropriately inform decision-makers and position the organization to those physical, operational, and technical deficiencies that pose the highest risk to the information assets within the enterprise. When approaching a risk management plan, it is important to develop an effective risk assessment that begins with identifying potential risks. When identifying potential cybersecurity risks it is important to identify both core and mission-critical functions and processes, develop an inventory of vulnerable assets associated with the core functions and processes, and assign a risk-impact score to each vulnerable asset (Chon et al., 2019). In addition to identifying potential IT vulnerabilities, risk determination can also be a valuable step when identifying potential threats. Statistical models such as the Bayesian probability model and Leontief-based model can be used to calculate the likelihood of attacks on certain components of the system and qualitative methods, such as conceptual diagrams and graphs demonstrated in figure 1, can provide a holistic overview of potential risks (Ren et al.,2017). Once each risk is identified and mission-critical assets and vulnerabilities are determined for each individual sector of the organization, a risk assessment is developed based on the likelihood of an adverse event, the impact of that event occurs, and any safeguards currently in place to reduce the effect of the occurrence. The following step in the process is mitigation planning, where a specific step is identified, a person is made responsible, and due date is assigned. The activity is then monitored, and a revised assessment of the risk is made following the mitigation (Bhuyan et al., 2020). It is important to realize that risk management is an ongoing, individualized discipline wherein each individual or each organization examines its threats, vulnerabilities, and valued assets and decides how to deal with each threat. Lastly, When developing an overall strategy for managing risks both internal and external factors must be continuously observed and identified by an organization (Saba & McCormick, 2015).

4.2.2 Second Layer: Information Assurance Policy

The risk management strategy will identify what risks need to be addressed through an information assurance policy that governs operations, information technology, and individual behavior. The information assurance policy is comprised of a standard set of rules and procedures that help to guide organizational decision-making and assist in defining behavioral expectations and establishing sanctions for unacceptable actions (Ren et al., 2017). The policy sets forth rules for protecting individuals' private information, for securing all confidential information, and for providing choice and transparency concerning how individuals' health information is used and shared. It is also comprised of rules that protect patients and their family members from physical harm that could result from data corruption or service interruption. It also defines the rules enforced to protect the organization's valued information assets from identified risks to the confidentiality, data integrity, and service availability. Although some policies are mandated by applicable state and federal laws and regulations, This HIT information assurance policy provides the foundation for the development and implementation of physical, operational, architectural, and security technology safeguards (Cuenca, 2017; Gade & Reddy, 2014).

4.2.3 Layer 3: Physical Safeguards

The physical safeguarding of health information and the IT used to collect, store, retrieve, analyze, and exchange health data is essential to assuring that information needed at the point of care is available, trustworthy, and usable in providing a high quality of care. Although the digital signals that represent health data are not in itself physical, the facilities which data are generated, stored, displayed, and used; the media on which data are recorded; the information system hardware used to display the data; and the communications equipment used to transmit the data are. Physical safeguards are essential to protecting these assets following the information assurance policy (Ren et al., 2017). The HIPAA Security Rule prescribes four standards for physically safeguarding electronic health information, which includes facility-access controls; workstation-use policies and procedures; workstation-security measures; and device and media controls (Cuenca, 2017). Healthcare organizations must include and adhere to the standards set forth by HIPAA when developing and maintaining a physical safeguard framework in-house or outsourcing these services from third parties. If an organization chooses to purchase these services from a third-party vendor, the organization must sign a business associate agreement in which they agree to meet all the HIPAA security standards. This agreement services in case a breach does occur; the covered entity retains primary responsibility for reporting and responding to the breach and can serve as a protective layer for the organization (Ren et al., 2017).

4.2.4 Layer 4: Operational Safeguards

Operational safeguards include processes, procedures, and practices that govern the creation, handling, usage, and sharing of health information under the information assurance policy. The processes, procedures, and practices that are included in the HIT trust framework are listed below with a detailed description of how to successfully implement them within the framework.

4.2.5 Layer 5: Architectural Safeguards

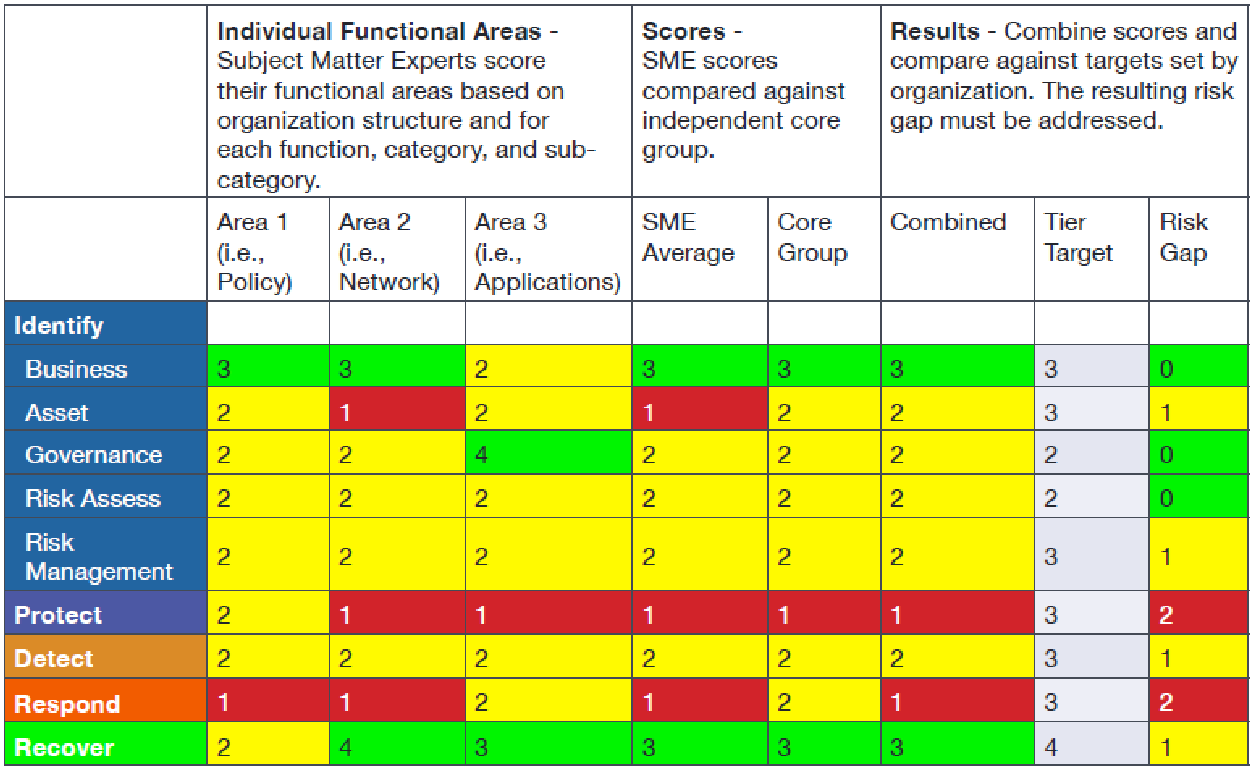
A system's architecture consists of individual hardware and software components, the relationships among them, their relationship within the environment, and the principles that govern the system's design and growth over time (Marianna et al., 2018). Specific architectural design principles, and the hardware and software components that support those principles, work together to establish a foundation for security technology safeguards. Whether an organization's enterprise architecture is centralized or distributed, the design principles that an organization needs to implement a plan for including future scalability, Reliability, safety, interoperability, availability, and process isolation among a system with different levels of authorization (Saba & McCormick, 2015).

4.2.6 Layer 6: Security Technology Safeguards

Security technology safeguards are software and hardware services specifically designed to perform security-related functions. These services include person and entity authentication, access control services, security audit controls, data integrity services, Non-repudiation of data through digital signatures, appropriate encryption processes, malicious software protection, and transmission security. All of these security technology safeguards need to be planned upon and implemented within an organization's security framework to properly secure patient health information and prevent data breaches (Saba & McCormick, 2015).

4.2.7 Layer 7: Usability Features

The final layer of the trust framework includes services that make life easier for end-users. Both single sign-on and identity federation enables a user to authenticate themselves only once to access multiple applications, multiple databases, and even multiple enterprises for which they are authorized, without having to re-authenticate. A key consideration for an organization to recognize is that these usability features do not actually provide increased security, and can inversely propagate security vulnerabilities within a system if earlier identity-proofing and authentication methods were poorly implemented (Saba & McCormick, 2015).



	Individual Functional Areas - Subject Matter Experts score their functional areas based on organization structure and for each function, category, and sub-category.			**Scores** - SME scores compared against independent core group.		**Results** - Combine scores and compare against targets set by organization. The resulting risk gap must be addressed.		
	Area 1 (i.e., Policy)	Area 2 (i.e., Network)	Area 3 (i.e., Applications)	SME Average	Core Group	Combined	Tier Target	Risk Gap
Identify								
Business	3	3	2	3	3	3	3	0
Asset	2	1	2	1	2	2	3	1
Governance	2	2	4	2	2	2	2	0
Risk Assess	2	2	2	2	2	2	2	0
Risk Management	2	2	2	2	2	2	3	1
Protect	2	1	1	1	1	1	3	2
Detect	2	2	2	2	2	2	3	1
Respond	1	1	2	1	2	1	3	2
Recover	2	4	3	3	3	3	4	1

Adapted from 'The Cybersecurity Framework in Action: An Intel Use Case'

Figure 1: Risk assessment impact scorecard

The above risk assessment impact scorecard is based on the current NIST cybersecurity framework and can be used by any healthcare organization looking to adopt this into their risk management implementation plan. It demonstrates how some cyber threats can be scored based on vulnerability and risk status and off specified core functions important to a specific organization.

Source: (Mindykowski et al., 2016)

4.3 Security Operations Management

HIPAA regulations require that each healthcare organization designate security and a privacy official to be responsible for developing and implementing security and privacy policies and procedures. When focusing on the management of services relating to the protection of health information and patient privacy it is important to consider that these services integrate with every function within a healthcare organization (Saba & McCormick, 2015).

4.4 Awareness and Training

One of the most valuable actions a healthcare organization can take to maintain public trust is to build a culture of safety, privacy, and security among their staff. If every person employed by an organization feels individually responsible for protecting the integrity and confidentiality of their patient's information, the risk for that organization can be drastically reduced. Recognition of the value of workforce training is reflected within the HIPAA Security and Privacy Rules and is why formal privacy and security training should be required to be completed at least annually (Argaw et al., 2020).

4.5 Configuration Management

Configuration management refers to processes and procedures for maintaining an accurate and consistent accounting of the physical and functional attributes of a system throughout its life cycle. This includes the controlling and detailed documentation of any hardware, software, and firmware consistently.

4.6 Identity Management and Authorization

These are the processes used to positively establish the identity of the individuals and entities to whom rights, and privileges are being assigned, and the process used to assign authorizations. Many of the technical safeguards rely upon the assumption and accuracy of an identity that is established when an account is created. This process should be completed using one or more government-issued documents containing the individual's photograph, or other proof of identity. Once identity has been positively established, system accounts are created, giving the individual the access rights and privileges essential to performing their assigned duties. Once the life cycle of that individuals' duties, or employment, has concluded within that organization a prompt termination of any authorization and privileges within the system should occur (Bhuyan et al., 2020).

4.7 Continuity of Operations

Unexpected events do happen, and when they do, it is important that critical health services can continue to be provided. As the dependence on electronic health information and information systems increases, the need to plan for unexpected events and the need to develop operational procedures that will enable the organization to continue to function becomes more urgent. Contingency planning is correlated with an effective risk-management strategy and should include architectural safeguards such as fail-safe design, redundancy and failover, and availability engineering (Saba & McCormick, 2015).

4.8 Incident Procedures

Awareness and training should include a clear explanation of what an individual should do if they suspect a security incident, such as a malicious code infiltration or a breach of confidential information. Organizations need to plan their response to an incident report, including procedures for investigating and resolving the incident, notifying individuals whose health information may have been exposed because of the incident, and penalizing parties responsible for the incident.

5. Conclusion

5.1 Develop A Response plan

It is hard to catch and gauge the genuine effect of the cyberattack. To forestall or moderate these sorts of occasions from repeating in the NHS or some other medical services association, there is a need to create and test effective incident management strategies and improve business congruity arranging. All associations should have the option to securely and adequately work while under cyberattack. In the interim, all information and frameworks should be safely supported up and catastrophe recuperation measures tried to guarantee that the reinforcement is secluded and cannot be eradicated or messed with (Jalali, Kaiser, 2018). Solid authority and a security culture all through the medical services area can help altogether to improve patient safety.

In an article from the Journal of the American Medical Informatics Association, to stay away from redundancy, 8 methodologies were proposed, making the eight aggregated response strategies (EARS) framework. EARS is intended to be utilized by network protection experts and chiefs in medical services associations (Jalali, Russell & Razak, 2019). This system gives methodologies that will help in pre-occurrence and post-episode response techniques. The most well-known covering suggestion remembered for the EARS structure was the contribution of key staff inside the association. For a visual introduction of the EARS system, see Figure 5. The eight response proposals were arranged into administrative and innovative classification; then components of the 8 recommendations (R1-R8) were divided into pre-and post-occurrence activities (Jalali, Russell & Razak 2019). R1-R5a. are for the most part pre-episode actions:

R1. An occurrence reaction plan should be built before a breach.

R2. Data security strategies are shown to energize the revealing of the episodes and empower the announcing of the seriousness of the occurrences whenever executed before a breach.

R3. The contribution of key faculty inside the association such as the Key staff and groups must have a strong comprehension of Pre-occurrence methodology and correspondences.

R4. Customary counterfeit testing of recuperation plans implies regular testing before an attack ought to be led on reinforcements and Therapeutic devices.

R5a. Contain the breach and forestall further spreading by isolating the clinical and clinic network through VLAN and air gapping; and Examination of devices before connection to the medical network.

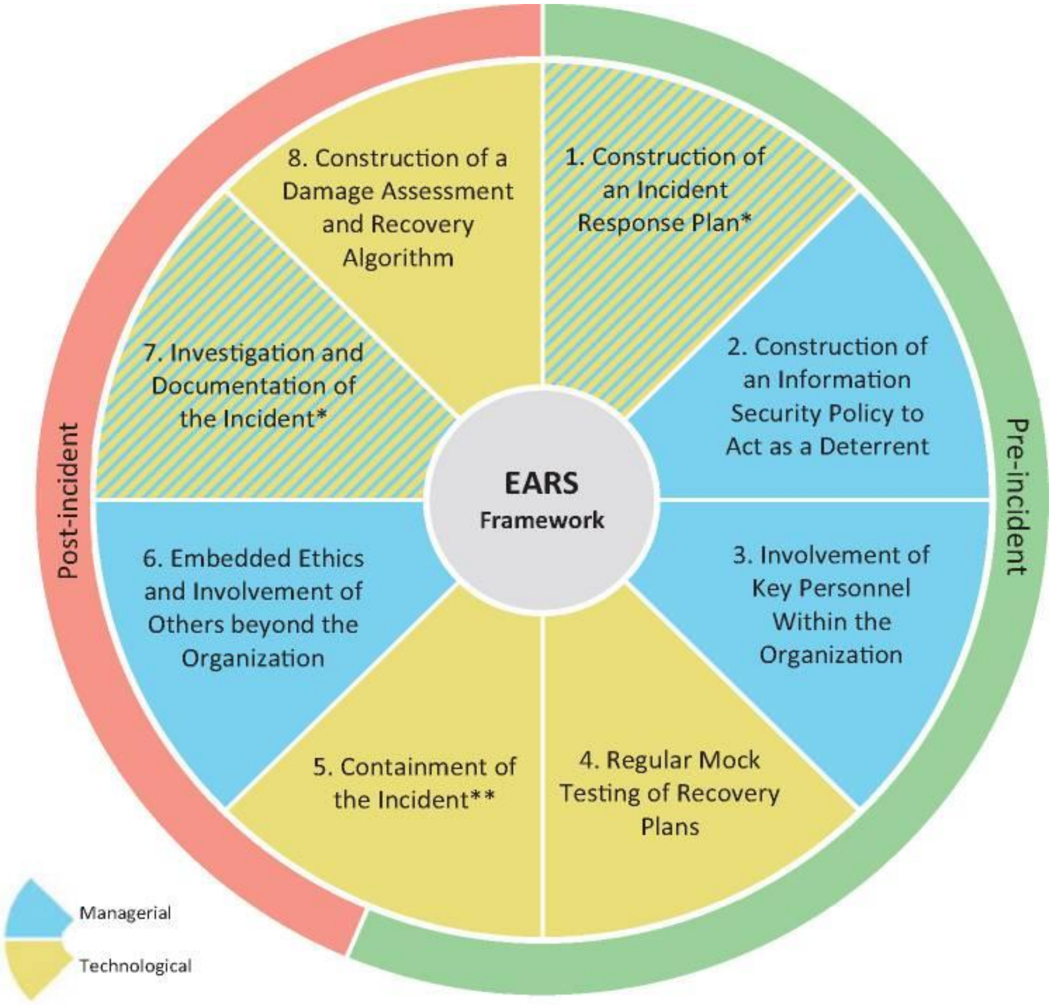
While R5b. – R8 are all post-incident actions:

R5b. Contain the occurrence and forestall additionally spread by killing every single contaminated device, disengage any tainted device from the organization, and Shut down the whole organization if under a far-reaching attack.

R6. Response to a breach should have the option to support moral qualities:

R7. Examination and documentation of the occurrence

R8. Development of a harm evaluation calculation and recuperation calculation.


EARS
Framework
1. Construction of an Incident Response Plan*
2. Construction of an Information Security Policy to Act as a Deterrent
3. Involvement of Key Personnel Within the Organization
4. Regular Mock Testing of Recovery Plans
5. Containment of the Incident**
6. Embedded Ethics and Involvement of Others beyond the Organization
7. Investigation and Documentation of the Incident*
8. Construction of a Damage Assessment and Recovery Algorithm
Pre-incident
Post-incident
Managerial
Technological

As every association is extraordinary, the proposals should be customized to the association. It must be noticed that an association needs to persistently create and alter its response plan to coordinate with the speed of advancing cybersecurity risks. The execution of EARS for a data breach in a medical care association can give the design to a cybersecurity response strategy.

5.2 AHA six-step plans to Cybersecurity.

With the various recent incidents of data breaches and security threats within healthcare facilities all over the country, healthcare facilities are more mindful of the increasing need to implement a comprehensive cybersecurity plan. The American Hospital Association (AHA) encourages its affiliates to engage in cybersecurity by using the AHA step plan as an aid to ensure cybersecurity with their facilities and organization These steps include the following.

Implement a comprehensive cybersecurity strategy in the event of an attack: conduct a thorough investigation into the incident (type of cyberattack, identification of compromised devices, review of entry points and vulnerabilities, warn and cooperate closely with authorities), provide specialist assistance where necessary, and take suitable corrective action toward non-compliant staff. According to the AHA, hospitals should consider joining regional or national information-sharing networks and learn all about the cybersecurity threats they pose besides senior management should be mindful about all the risks they face by using their IT and learn how to mitigate them via compliant usage.

End-users must ensure that all software is up to date and that their devices are secured with the appropriate firewalls and antiviruses. They will also provide quick updates to the vendor by tracking the device's activity such as glitches, unauthorized accesses, and attack attempts, along with full reports on the method and potential success.

Create a specialized team whose priority will be to investigate the existing state of the facility's cybersecurity, develop procedures to strengthen it, and minimize vulnerabilities as often as practicable. Set aside a portion of the budget to increase awareness, educate staff, and monitor their progress macro-management (Kwon, & Johnson 2013).

6. Recommendations

6.1 Managing Cybersecurity risk

In the last few decades, technological advancement and global interconnectivity have accelerated. Although the growth of information technology has many advantages, it also has disastrous implications in terms of "advanced persistent threats, DDoS (Distributed Denial of Service) attacks, ransomware breaches, cyber espionage, and computer and intellectual property theft. Most especially within the healthcare system, the healthcare sector is especially vulnerable to the consequences of improper use of personal and confidential data (Micro,2013) .

Hackers invading personal privacy regularly, and selling stolen identities on the black market, is a common occurrence. The rampant degree of cybersecurity risks and threats within the healthcare system can jeopardize hospital information technology (IT) networks and medical equipment operation since the system lags behind other leading sectors in protecting vital records, the healthcare sector is a prime target for all forms of patient information fraud. Hackers invading personal privacy regularly, and selling stolen identities on the black market, is a common occurrence. According to the Ponemon Institute in the year 2015, about 90% of health institutions have suffered a cyber-attack since 2012. These attacks targeted patient records, billing, and insurance data repositories, and the trend is expected to continue as most healthcare data continue to be stored electronically (Brady, 2011).

In managing security risks all practitioners and personnel within the healthcare system are directly or indirectly responsible which in turn gives every individual within the healthcare system a sense of accountability when a potential breach is evident within the system. It is a well-known fact that most data comptonization that takes place within healthcare are mostly as a result of human error, Hackers take advantage of common but costly mistakes made by personnel's within the healthcare facility to use as an easy route to gain unauthorized access into the internal systems through emails and unexpected phishing attacks in other to be ahead of these potential threats in the Management of Cybersecurity risks there should be a high rate of security awareness which can be achieved through the following steps as mentioned below:

- All personnel and team members within the organization must be educated on not just how to secure the organization's assets but also their security outside of the workplace which makes it personal, which will aid the creation of a security culture within the Healthcare facility as staff members will apply what they have been taught effortlessly.
- There should be a continuous assessment of the effectiveness of the security awareness Training through unexpected periodic social engineering and phishing in combination with employee empowerment.
- Team members and personnel within the system should be encouraged to speak up and ask questions without fear of repercussions, when this measure is imbibed into the fabric of the system, employees will be more forthcoming in reporting errors before it is the situation is beyond redemption.
- There should be a critical focus on access authorization and management within the organization regardless of the size, although larger and more established facilities tend to excel in identity management, which might include measures such as incorporating new technology like retinal or other biometric screening solutions, the startup or smaller facilities also need to have systems in place for access management as data security within the healthcare system cycles through interoperability. In other words, if access and authorization are not properly managed in a smaller facility, they could expose the larger facility to a data breach to sharing of compromised data (Conn,2013).

6.2 Guidelines

The data that health providers, technology vendors, and those who handle medical data are in charge of is very vulnerable. Health data managers have a responsibility to ensure that the data they maintain is safe from theft, carelessness, or providing unintended access by mistake. Dependent on the country or state, the rules for security conditions vary within the healthcare system. ISO 27001 which is internationally applicable, and HIPAA (Health Insurance Portability and Accountability Act) are two similar sets of standards (applicable in the United States). ISO 27799 and the HITRUST Common Security Framework are two security principles that can be used that have more direct rules than guidance, while there is a lot of variation between these two sets of security guidelines, they each have their own set of specifications (DeZabala, Saif, & Westermann,2011).

The Healthcare Insurance Portability and Accountability; In 1996 HIPAA was signed into law to enhance the accountability and portability of health insurance coverage. This was the beginning of the government's drive for the computerization of health information, which led to the HIPAA Privacy and Security Regulations, which regulated how institutions protect handled patient data. The HIPAA Privacy and Protection Rules define a set of security requirements that "protected institutions" must adhere to, which are divided into four sections: Enforcement Rule, Breach Notification Rule, Privacy Rule, and Security Rule.

ISO 27001 / ISO 27799; ISO 27001, which defines information security management system guidelines, and ISO 27799, which is a compilation of best practices explicitly created for dealing with health records, are two international security standards that can be applied in conjunction with one another to discuss the privacy of confidential health information.

HITRUST Common Security Framework; The HITRUST CSF is a broad structure that maps to several security specifications to include an encompassed step for meeting the criteria laid out by ISO, HIPAA, NIST, and PCI. The aim of the HITRUST CSF is for protected bodies to meet the criteria laid out in the CSF's 19 realms and 135 basic controls, or activities. Covered organizations can conveniently respond to audit demands for any of the compliance specifications that the CSF maps to by meeting these requirements, saving time and resources from both the purchaser and vendor sides (HITRUST Alliance ,2014).

6.3 Solution

At the end of the day, Cybersecurity in healthcare is important now than ever for the smooth delivery of healthcare services with the emergence of new diseases that we see today, policies, regulations, and restrictions are not enough to ensure the security of sensitive health data. In addition to all of the already mentioned measures the following measures will also aid optimized data security in healthcare they include the following;

Creation of a ransomware policy; a single breached or disabled system might not necessarily bring major damage however, the inability to enter wider sectors where electronic records are stored may be detrimental, if not harmful, to the whole internal system within the health care facility. Employees must urgently call someone on their healthcare IT team if such an incident occurs this should be part of their overall security awareness and training. Instead of trying to fix these potential threats on their own, protocols and procedures must be followed immediately after a potential threat is detected. Authorities advise against paying ransomware attackers since there is no assurance that an attach will be reversed, Law enforcement should be immediately contacted in the event of a ransomware attack besides cloud data backups will make it simple to rebuild networks, disaster recovery planning should be done before a cybersecurity threat occurs (Filkins,2014).

Cybersecurity needs to be extended beyond employee access; When designing safer, secure solutions or developing cybersecurity mechanisms, patient questions about confidential data protection and IT in healthcare should be kept in mind if a hospital's security is compromised, patients are often worried and don't want to know about data security. Threat intelligence support should be a conjoined effort of both the healthcare facility and the patient as well as security consciousness is both the responsibility of the healthcare facility as well as the patients.

Data cloud migration should be encouraged; The cloud is a reliable and versatile approach for healthcare data collection and backup. It also allows for on-demand scaling of services, which can significantly change the way healthcare organizations handle their data and in the event of a breach or interruption, cloud-based storage and disaster recovery tools ensure that patient records are secure. By using the cloud, a healthcare institution can save money on sensitive resources and data management. Since no hardware upgrades are needed, HIPAA Compliant Cloud Storage allows for substantial IT cost savings. It also adds a new degree of versatility to an institution's operations.

Ensure vendor's compliance is taken seriously; The Healthcare Industry Cybersecurity Task Force, which was formed by the US Departments of Health and Human Services and Homeland Security, cautioned healthcare providers about supply chain vulnerabilities. One of their regulation is that providers take appropriate measures to track and identify risks, as well as to restrict access to their networks. To secure patient documents, insurance agencies, infrastructure contractors, and all other healthcare industry partners must have spotless security records. Before any Health care Organization enlists the service of any vendor the security measures of such vendor should be put under extreme scrutiny to ensure there is an optimized security measure in place (Gikas,2010).

6.4 Valuing Cybersecurity Risks and Mitigating Measures

Cyber-attacks in healthcare have become increasingly exorbitant and growing more frequent, putting user and patient data at risk. And with the rapid adoption of health information technology coupled with the growing reports no healthcare organization, regardless of size, is insusceptible from the data breach (Jalali, Kaiser, 2018). To estimate these costs a thorough investigation must be conducted that for a period longer than the 8 weeks given for this research. Such studies include the one by the Ponemon Institute that examined the costs sustained by 277 companies in 16 different healthcare industry sectors after those companies experienced the loss or theft of protected personal data (Ponemon Institute, 2013).

The cost presented in the research were all actual not theoretical data loss incidents that were based on cost estimates provided by the companies interviewed over ten months. According to the study, nearly 90 percent of healthcare organizations studied had a data breach and nearly half or 45 percent had more than five data breaches at the same period. Based on that, it is estimated that data breaches could cost a healthcare industry a total of $5.4 million (Ponemon Institute, 2013). This is calculated by collecting both the direct and indirect expenses incurred by the organization. Direct expenses include drawing in forensic specialists, rethinking hotline support, and giving free credit observation memberships and discounts on future items and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates (Gode, 2014).

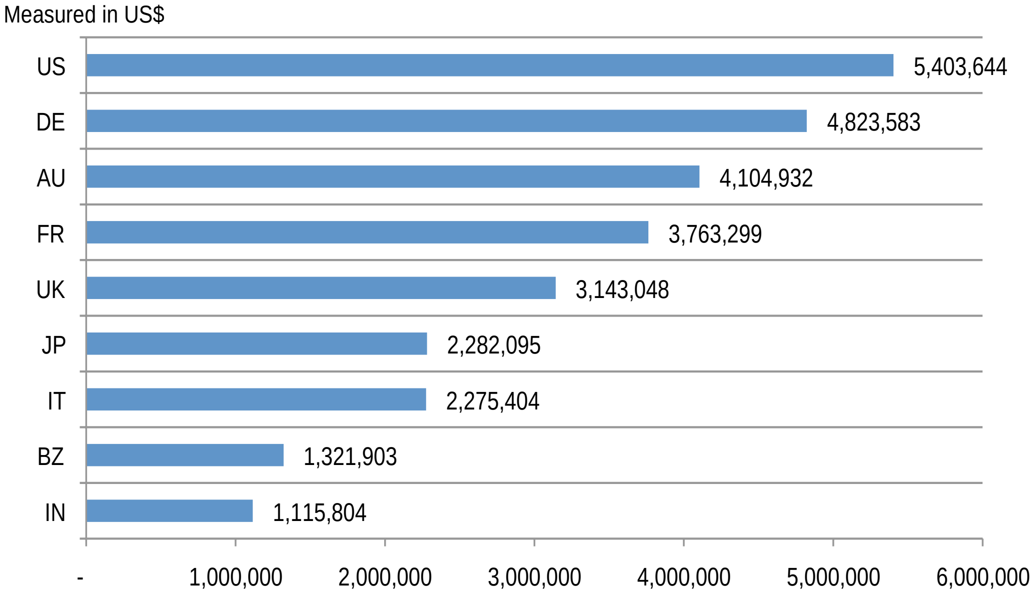


Figure 2: The average total organizational cost of the data breach

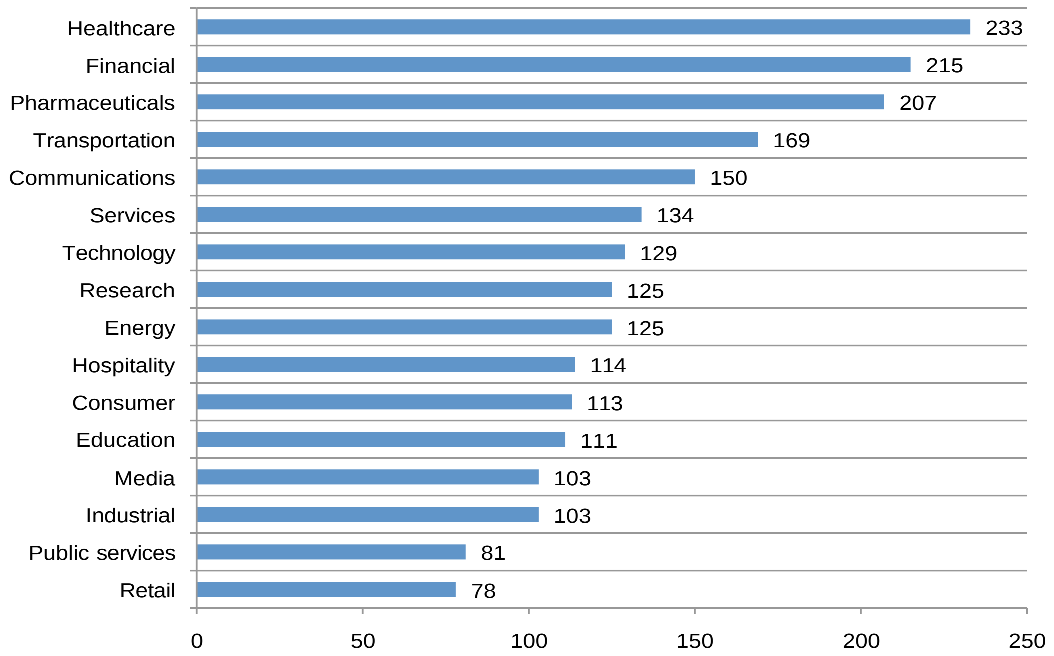


Figure 3: Per capita cost by industry classification

The figures above illustrate the result from the study by Ponemon Institute in the 2013 edition of the Cost of Data Breach Study: Global Analysis; a mention the study focused on 277 companies in 16 different healthcare industry sectors. Figure 2 shows the total average cost of a data breach for nine country studies in this year's study. The United States experienced the highest total average cost at followed by Germany at $4.8 million. Figure 3 gives deeper into to the industry classification's per capita cost which is defined as the total cost of data breach divided by the size of the data breach in terms of the number of lost or stolen records (Ponemon Institute, 2013). So, the higher the number of lost or stolen records, the more the total cost of the data breach.

Cooperation number= 277

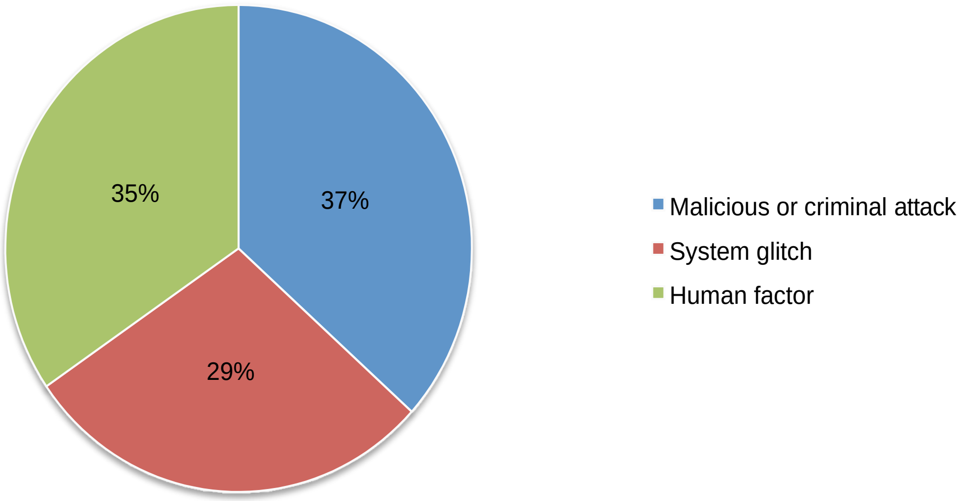


Figure 4: Distribution of the benchmark sample by the root cause of the data breach

Figure 4 explains the main root causes of cyber-attacks on the companies studied. Results show over 37 percent of cases involved a malicious or criminal attack which can include malware infections, criminal insiders, phishing/social engineering, and SQL injection. These types of attacks can hackers or criminal insiders such as employees, contractors or other third parties making the second root cause of data breach 35 percent a negligent employee or contractor (human factor), and the remaining 29 percent stemming from system glitches that include both IT and business process failures (Ponemon Institute, 2013).

To mitigate the cost measures, the health industry must work to decrease the number of lost or stolen records. In order words, both user and patient must work effectively against data t, in response to heft. Educating patients and employees in cyber safety is one keyway to begin (Arain, Tarraf,& Ahmad, 2019). According to an article, in response to a virus attack that had the main root cause of human factor the Michael Garron Hospital in Toronto required all staff to take further training in cybersecurity and strengthen its firewall these steps can reduce the risk of future incidents substantially for many hospitals (Owens, 2020).

Another thing to consider is the Investments in cybersecurity spending amounts companies are making and the quality of their cybersecurity programs. Based on Ponemon Institute 2017 Cost of Cyber Crime Study, to comprehend the adequacy of investment decisions, nine security innovations were investigated more readily across two measurements: the rate spending level among them and their worth as far as cost-reserve funds to the business. The discoveries show that numerous associations might be spending a lot on some unacceptable advances. Five of the nine security technologies had a negative worth gap where the rate spending level is higher than the general worth to the business. Of the leftover four technologies, three had a critical positive worth gap and one was in balance (Ponemon Institute, 2017). In this way, while keeping up the state of affairs on cutting edge personality and access administration, the chance exists to assess potential over-spend in regions that have a pessimistic worth gap and rebalance these assets by putting resources into the advancement developments which convey positive value. The study advised that the establishment of a solid and successful security program is to distinguish and "solidify" the higher-esteem resources. These are the royal gems of a business the resources generally basic to activities, subject to the most rigid administrative punishments, and the source of significant proprietary advantages and market separation. Solidifying these resources makes it as troublesome and exorbitant as workable for foes to accomplish their objectives and limits the harm they can cause if they do get access.

According to the study, the average annualized cost of cybersecurity $11.7 million; it explains that Associations need to perceive that cost alone does not continuously compare to the value. Past avoidance and remediation, if the security falls flat, organizations face surprising expenses from not being ready to maintain their organizations effectively to contend in the advanced economy. Knowing which resources should be secured, and what the results will be for the business if assurance fails, requires a canny security procedure that forms versatility from within and an industry-explicit methodology that secures the whole worth chain (Ponemon Institute, 2017).

Figure 5 below, according to Ponemon Institute's research results shows the cost organizations can save by sending every one of seven empowering security innovations. For instance, companies utilizing security intelligence systems experienced a significant expense investment funds of US $2.8 million. Also, organizations conveying progressed personality and access administration devices experience cost reserve funds of US $2.4 million overall. While not broadly utilized, computerization, association, and AI (machine learning) can give tremendous expense reserve funds (a normal of US$2.4 million). Also noted that these extrapolated cost investment funds are free of one another and cannot be added together.

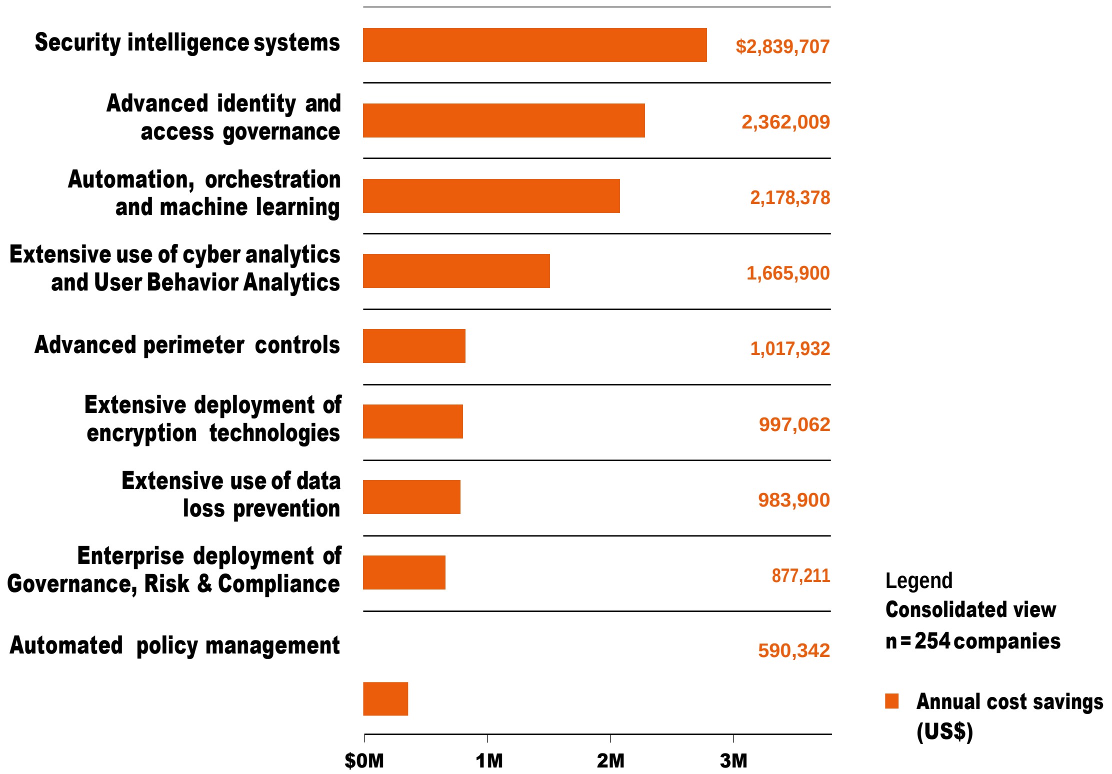


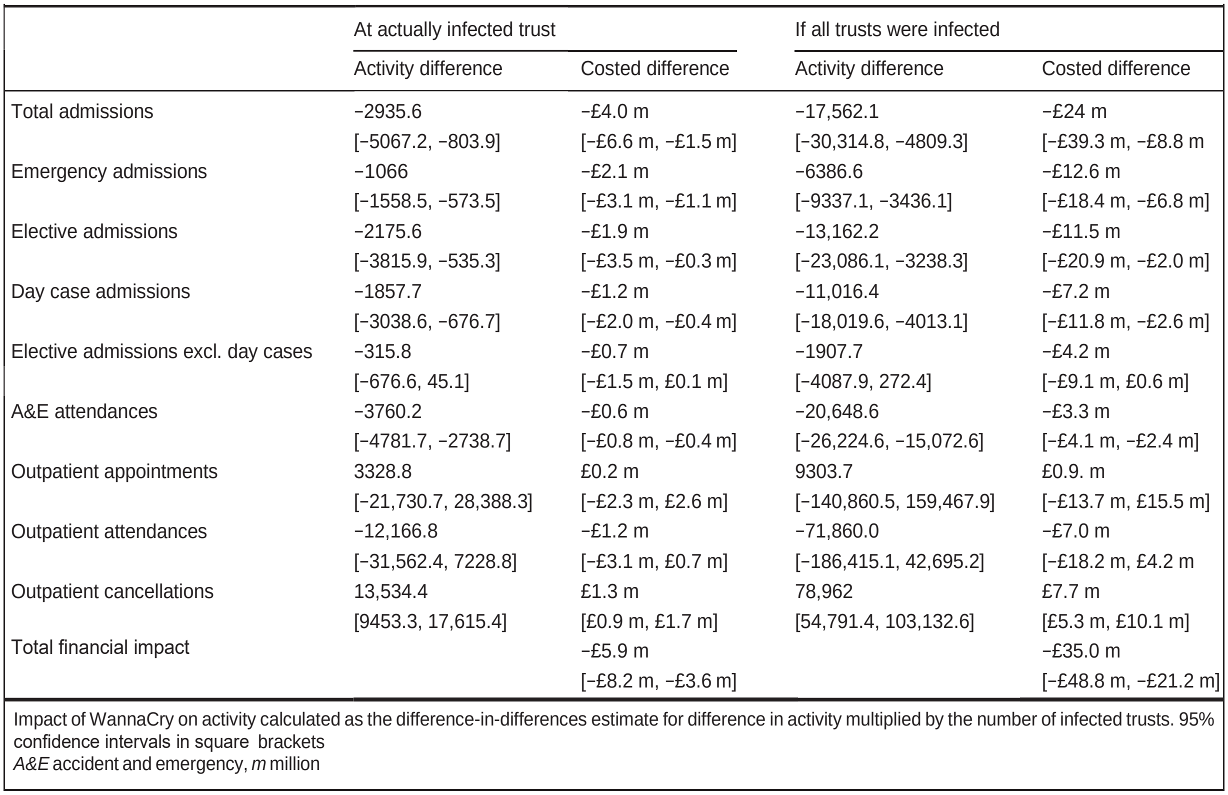
Figure 5: Cost savings when deploying enabling technologies

6.5 Estimating Negative Outcomes from Different Attack Scenarios.

Quite possibly the latest cyberattack experienced internationally was the May 2017 worldwide WannaCry attack (Ghafur, Kristensen, Honeyford, et al., 2019). This was a ransomware worm that spread quickly across various PC networks comprising of different segments. It shows up on the tainted PC as a dropper, an independent program that separates the other application segments inserted inside itself. Segments include an application that encodes and decodes the information, documents containing encryption keys, and a copy of Tor (which is short for The Onion Router and was at first an overall organization of workers created with the U.S. Naval force that empowered individuals to peruse the web secretly. Presently, it is a non-profit association whose fundamental reason for existing is the innovative work of online security apparatuses) (Jadoon, Iqbal, Amjad, et al.,2019). The program code is not jumbled and was generally simple for security professionals to examine. Once dispatched, WannaCry attempts to get to a hard-coded URL, if it cannot, it continues to look for and encode records in many significant arrangements, going from Microsoft Office documents to MP3s and MKVs, leaving them unavailable to the client. It at that point shows a payment notice, requesting $300 in Bitcoin to decode the records (Ghafur, Kristensen, Honeyford, et al., 2019).

The researchers explained to look at the general effect of the WannaCry assault on public movement, a model looking at normal action per trust each day during the WannaCry week and the month encompassing the seven days of the assault to action during the gauge time frame, which was some other week between 1 April and 30 June 2017 was assessed. Likewise, to comprehend the effect of WannaCry on all-out public action, the anticipated action from the scientist's model was contrasted with the forecasts of all-out public movement if action during the WannaCry week had been like the pattern weeks. The assessed coefficients consequently mirror the normal distinction in day-by-day movement across all emergency clinics in weeks prior, during, and after WannaCry contrasted with the standard. Dummy variables were also included for the day of the week, bank occasion, and medical clinic fixed impacts. To study the effect on activity explicitly at the contaminated trusts, the researchers compared the adjustment of every outcome at the infected facilities to the adjustment of those results at the non-infected facilities in a distinction in contrasts approach utilizing common least squares. In all models, the analysts included controlled factors for day of the week and bank occasions and utilized hospital fixed impacts to control for unseen time-invariant contrasts between hospitals. The distinction in action between hospitals that were influenced and those neither influenced nor infected was additionally tested.

While assessing all post impact on infected hospitals, it was anticipated the normal movement of the Wanna Cry week had been like the baseline weeks at the contaminated hospitals and analogized the gauge of complete activity with the real activity at the contaminated trusts. The researchers also determined the normal effect if all hospitals had been tainted and determined the contrast among genuine and anticipated activity under this situation. The monetary effect of WannaCry was estimated at actually and possibly tainted hospitals by multiplying the total activity impact estimates with average tariffs for the specific type of activity.



	At actually infected trust		If all trusts were infected	
	Activity difference	Costed difference	Activity difference	Costed difference
Total admissions	−2935.6	−£4.0 m	−17,562.1	−£24 m
	[−5067.2, −803.9]	[−£6.6 m, −£1.5 m]	[−30,314.8, −4809.3]	[−£39.3 m, −£8.8 m
Emergency admissions	−1066	−£2.1 m	−6386.6	−£12.6 m
	[−1558.5, −573.5]	[−£3.1 m, −£1.1 m]	[−9337.1, −3436.1]	[−£18.4 m, −£6.8 m]
Elective admissions	−2175.6	−£1.9 m	−13,162.2	−£11.5 m
	[−3815.9, −535.3]	[−£3.5 m, −£0.3 m]	[−23,086.1, −3238.3]	[−£20.9 m, −£2.0 m]
Day case admissions	−1857.7	−£1.2 m	−11,016.4	−£7.2 m
	[−3038.6, −676.7]	[−£2.0 m, −£0.4 m]	[−18,019.6, −4013.1]	[−£11.8 m, −£2.6 m]
Elective admissions excl. day cases	−315.8	−£0.7 m	−1907.7	−£4.2 m
	[−676.6, 45.1]	[−£1.5 m, £0.1 m]	[−4087.9, 272.4]	[−£9.1 m, £0.6 m]
A&E attendances	−3760.2	−£0.6 m	−20,648.6	−£3.3 m
	[−4781.7, −2738.7]	[−£0.8 m, −£0.4 m]	[−26,224.6, −15,072.6]	[−£4.1 m, −£2.4 m]
Outpatient appointments	3328.8	£0.2 m	9303.7	£0.9. m
	[−21,730.7, 28,388.3]	[−£2.3 m, £2.6 m]	[−140,860.5, 159,467.9]	[−£13.7 m, £15.5 m]
Outpatient attendances	−12,166.8	−£1.2 m	−71,860.0	−£7.0 m
	[−31,562.4, 7228.8]	[−£3.1 m, £0.7 m]	[−186,415.1, 42,695.2]	[−£18.2 m, £4.2 m
Outpatient cancellations	13,534.4	£1.3 m	78,962	£7.7 m
	[9453.3, 17,615.4]	[£0.9 m, £1.7 m]	[54,791.4, 103,132.6]	[£5.3 m, £10.1 m]
Total financial impact		−£5.9 m		−£35.0 m
		[−£8.2 m, −£3.6 m]		[−£48.8 m, −£21.2 m]

Impact of WannaCry on activity calculated as the difference-in-differences estimate for difference in activity multiplied by the number of infected trusts. 95% confidence intervals in square brackets
A&E accident and emergency, *m* million

Table 1: The estimated impact of WannaCry on total activity during the WannaCry week

Table 1 illustrates the outcomes from an article NPJ Computerized Medication published enumerating Activity totals determined for every one of the results a long time previously (weeks), during, and after the WannaCry attack. then the week of the WannaCry attacks was characterized as the 7 days after and including the main day of the assault. The all-out monetary estimation of the lower action at the contaminated trusts during the WannaCry week was £5.9 m (95% certainty stretch £3.6 m to £8.2 m), including £4 m (£1.5 m to £6.6 m) in lost inpatient confirmations, £0.6 m (£0.4 m to £0.8 m) from lost A&E action, and £1.3 m (£0.9 m to £1.7 m) from dropped outpatient arrangements (Ghafur, Kristensen, Honeyford, et al., 2019). Accepting that all trusts had been tainted by WannaCry and influenced to the equivalent stretch out as the contaminated trusts, the complete estimation of lost action might have added up to £35 m (£21.2 m to £48.8 m) in action alone.

7. References:

- Alharam, A. K., & El-Madany, W. (2017, May). The effects of cyber-security on healthcare industry. In 2017 9th IEEE-GCC Conference and Exhibition (GCCCE) (pp. 1-9). IEEE.
- Arain, M. A., Tarraf, R., & Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization.

Journal of multidisciplinary healthcare, 12, 73–81. https://doi.org/10.2147/JMDH.S183275

- Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., . . . Eshaya-Chauvin, B. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1), 1-10.
- Bhuyan, S.S., Kabir, U., Escareno, J.M. et al. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J Med Syst 44, 98 (2020). https://doi.org/10.1007/s10916-019-1507-y
- Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., . . . Dobalian, A. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J Med Syst, 44(5), 98. doi:10.1007/s10916-019-1507-y
- Bai, G., Jiang, J. X., & Flasher, R. (2017). Hospital Risk of Data Breaches. JAMA internal medicine, 177(6), 878–880. https://doi.org/10.1001/jamainternmed.2017.0336
- Bouazzaoui, S., & Daniels, C. (2020, March). Electronic Healthcare Record and Cyber Security Threats: A Development of an Agile Framework. In International Conference on Cyber Warfare and Security (pp. 67-XII). Academic Conferences International Limited.
- Bowman, S. (2013). Impact of electronic health record systems on information integrity: quality and safety implications. Perspect Health Inf Manag, 10(Fall), 1c.
- Brady, J. W. (2011). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. Proceedings of the 44th Hawaii International Conference on System Sciences (pp. 1-10). Kauai: IEEE. Civic Impulse. (2009). H.R. 1 — 111th Congress: American Recovery and Reinvestment Act of 2009. Retrieved from https://www.govtrack.us/congress/bills/111/hr1
- Camp, L. J. (2011). Reconceptualizing the Role of Security User. Daedalus, 140(4), 93-107. doi:10.1162/DAED_a_00117
- Chon, A., Dave, C., & Ronald, R. S. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons, 62(4), 539-548. doi: https://doi.org/10.1016/j.bushor.2019.03.010
- Conn, J. (2013, August 13). Advocate data breach highlights lack of encryption, a widespread issue. Modern Healthcare. Retrieved from http://www.modernhealthcare.com/article/20130830/NEWS/308309953
- Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.
- Cuenca, J. V. (2017). Cybersecurity Challenges in Healthcare Industries. Utica College,

- DeZabala, T., Saif, I., & Westermann, G. (2011, July 1). Evolve or fail. Deliotte University Press. Retrieved from http://dupress.com/articles/evolve-or-fail-how-security-can-keep-pace-with-strategy/
- Dogaru, D. I., & Dumitrache, I. (2017, June). Cyber security in healthcare networks. In 2017 E-Health and Bioengineering Conference (EHB) (pp. 414-417). IEEE.
- Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25, 55-63.
- Filkins, B. (2014). SANS health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon. Retrieved from http://www.sans.org/readingroom/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detectedcompliance-nightmare-horizon-34735
- Gade, N. R., & Reddy, U. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.
- Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ digital medicine, 2, 98. https://doi.org/10.1038/s41746-019-0161-6
- Gikas, C. (2010). A general comparison of FISMA, HIPPA, ISO 27000 and PCI-DSS standards. Information Security Journal: A Global Perspective, 19(3), 132-141.
- Gode, S. (2014). Increasing data breach costs should lead to a review of insurance policies and vendor contracts. Linkedin.com. Retrieved 26 April 2021, from https://www.linkedin.com/pulse/20140625132714-7012399-increasing-data-breach-costs-should-lead-to-a-review-of-insurance-policies-and-vendor-contracts?trk=portfolio_article-card_title
- HITRUST Alliance. (2014, July). Cyber threat intelligence and incident coordination center: Protecting the healthcare industry form cyber-attacks. Health Information Trust Alliance (HITRUST). Retrieved from http://hitrustalliance.net/content/uploads/2014/07/ HiTrustC3Datasheet.pdf
- Jadoon, A. K., Iqbal, W., Amjad, M. F., Afzal, H., & Bangash, Y. A. (2019). Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web. Forensic science international, 299, 59–73. https://doi.org/10.1016/j.forsciint.2019.03.030
- Jalali, M. S., Russell, B., Razak, S., & Gordon, W. J. (2019). EARS to cyber incidents in health care. Journal of the American Medical Informatics Association : JAMIA, 26(1), 81–90. https://doi.org/10.1093/jamia/ocy148
- Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of medical Internet research, 20(5), e10059. https://doi.org/10.2196/10059

- Judy, H.L., David, S.L., Hayes, B.S., Ritter, J.B., & Rotenberg, M. (2009). Privacy in cyberspace: U.S. and European perspectives. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), Computer security handbook (5th ed). New York, NY: John Wiley & Sons.
- Keizer, G. (2006). FBI Recovers Stolen Veterans Affairs Laptop. Retrieved from http://www.informationweek.com/fbi-recovers-stolen-veterans-affairs-laptop/d/d-id/1044759?
- Kwon, J. & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. Journal of the American Medical Informatics Association, 20(1), 44-47.
- Marianna, L., Mariangela, L., & Angelo, C. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97-110. doi: https://doi.org/10.1016/j.compind.2018.09.004
- Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? BMJ, 358.
- McCann, E. (2014, October 6). Missed Ebola diagnosis leads to debate. Healthcare IT News. Retrieved from http://www.healthcareitnews.com/news/epic-pushes-back-against-ebola-ehr-blame-shifting
- McDavid, S. (2014, March). A primer on cybersecurity litigation for the not-so-tech-savvy attorney. American Bar Association, 3(8), 17-19. Retrieved from http://www.americanbar.org/publications/gpsolo_ereport/2014/march_2014/primer_cybersecurity_ litigation_for_not-so-tech-savvy_attorney.html
- McGrory-Dixon, A. (2013). HHS toughens HIPAA violation penalties. Benefits Pro. Retrieved from http://www.benefitspro.com/2013/04/09/hhs-toughens-hipaa-violation-penalties
- Micro, T. (2013). VA records breach shows difficulty of balancing cyber security, physical security. Retrieved from http://blog.trendmicro.com/va-records-breach-shows-difficulty-balancing-cybersecurity-physical-security/
- Mindykowski, P., Honfi, D., Lange, D., Sjostrom, J., Cadete, G., Carreira, E., . . . Petersen, L. (2016). Physical exposure identification and mapping methodologies.
- Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intelligence and National Security, 35(4), 556-585.
- Ponemon Institute. (2013). 2013 Cost of Data Breach Study: Global Analysis. Ponemon.org. Retrieved 26 April 2021, from https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf
- Ponemon Institute. (2017). 2017 Cost of Cyber Crime Study: Insights On The Security Investments That Make A Difference. Retrieved 27 April 2021, from

https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

- Ren, A., Wu, D., Zhang, W., Terpenny, J., & Liu, P. (2017). Cyber security in smart manufacturing: Survey and challenges. IIE Annual Conference.Proceedings, , 716-721. Retrieved from https://www-proquest-com.marshall.idm.oclc.org/scholarly-journals/cyber-security-smart-manufacturing-survey/docview/1951124648/se-2?accountid=12281
- Saba, V. K., & McCormick, K. A. (2015). Essentials of nursing informatics (Sixth edition. ed.). New York: McGraw-Hill Education
- Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical devices (Auckland, N.Z.), 8, 305–316. https://doi.org/10.2147/MDER.S50048