Cyber Security threats and mitigations in the Healthcare sector

Wijesekara W.M.J.P (IT19961118)

Sri Lanka Institute of Information Technology

it19961118@my.sliit.lk

Abstract

A new generation of medical devices with improved sensing and actuation capabilities has emerged as a result of the Internet of Things. Preventive mitigation of cyber hazards that emerge in this hyperconnected world is necessary to ensure the long-term safety of patients.

Technology is becoming more integrated into the healthcare industry, which is helping to improve the precision of medical care; yet, network security still needs to be improved. However, network security improvements are still required. According to a 2016 research by IBM and the Ponemon Institute, data breaches in the healthcare industry have grown since 2010, making it one of the most hacked businesses in the world.

Due to the immutability of the information collected through health data breaches, criminals are particularly interested in it. The medical file of an individual contains information such as blood type, previous operations and diseases, and other personal health data.

When personal information is broken, it is impossible to restore privacy or reverse psychological injury because these records contain private data such as name, birth date, insurance, and health provider information, as well as health and genetic material.

Cyberattacks like these can compromise patients' identities and funds, as well as disrupt hospital operations and put their health and well-being at risk. Hospitals in the United Kingdom's National Health System were forced to postpone treatment plans and even detour inbound ambulances due to the WannaCry ransomware attacks in May 2017. Cyberattacks have long-term detrimental effects on hospitals' and health organizations' reputations and revenues, in addition to the operational delays and financial costs of data breaches and ransomware attacks.

Index Terms

MIoT - Medical Internet of Things

OPM - Office of Personnel Management

SQL - structured query language

MHR - My Health Record

Introduction

Health care is a basic human necessity that impacts everyone in society. The healthcare industry is in charge of collecting, preserving, and exchanging extremely sensitive and personal data with medical professionals, patients, and other organizations. The health-care system is under pressure to keep up with technological advances. The digitization of health records aids the inevitable and necessary shift in healthcare from a hospital-centric, expert-centric approach to patient-centric, dispersed care. [1] [2]

Patients and medical institutions will be harmed by HCS network security breaches that disclose critical information or data, and may even result in death. Ransomware assaults, [3]medical device hacking, and data theft are all increasing healthcare's cyber security concerns. Hacked health data is more valuable than any other

industry record because personal data is so important.

They're available on the dark web and may be used to finance crimes like identity theft, blackmail, and even murder. For example, the US Office of Personnel Management (OPM) and Anthem Wellness, which provides healthcare to federal employees, were both compromised by the same hacker within a few months of 2015. As a result, thieves will be able to link government employees' job records with critical health information, allowing them to damage high-value persons. Despite the rise in cyber assaults against healthcare institutions throughout the world, the healthcare business frequently falls behind other industries in terms of securing sensitive data. [4]

Despite the fact that cybersecurity in healthcare has been highlighted as a growing health and safety concern, there is a lack of understanding of the risks in the business. A plan for healthcare cybersecurity capabilities must be established in order to respond to the rising cyber threats. The recently established Australian National Electronic Medical Record My Health Record (MHR) allows healthcare networks to test their security capabilities.

Increasing cyber security capabilities necessitates not just upgrading present information infrastructure, but also anticipating and driving the demand for new technologies, cyber security insights, and rigorous organizational training. The use of information technology to store significant volumes of electronic patient data on multiple operating systems is required as part of the move to digital healthcare. Integrating new technologies with out-of-date, unsupported, or unsupported operating systems might jeopardize interoperability and raise cybersecurity risks. A excellent example is the worldwide WannaCry ransomware attack in 2017. [5] [6]

The virus propagated in the UK's National Health Service due to extensive usage of obsolete Windows XP programs and a refusal to upgrade the system's cybersecurity warnings (NHS). WannaCry was the most widespread ransomware attack to date, shutting down the NHS for a week from May 12 to 17, 2017, and impacting 200,000 systems in over 100 countries. WannaCry was able to spread to 80 out of 236 NHS trusts and 603 primary care organizations in England due to poor cyber hygiene and executive healthcare managers' lack of awareness of the business risk repercussions of cyber breaches.

Ambulances were diverted, test equipment was polluted, pathology and radiology were out of commission, patient records were unavailable, and over 7,000 medical appointments were cancelled. Healthcare is renowned for having a poor degree of security knowledge and a lack of contemporary data security procedures when compared to other businesses. Budget restrictions, a lack of network security training and awareness among health managers, many health information systems, and a significant number of wirelessly linked devices are all concerns. In the healthcare industry, cyber security is largely passive, with actions performed only after a malicious assault.

Network hazards have been worsened by the traceability of health network security and the industry's reliance on perimeter defenses (antivirus, firewall). Such protective methods are unlikely to tackle complex and persistent assaults or insider threats. The dearth of qualified network security professionals in the field, as well as changing malware threats and complicated network infrastructure, are all important obstacles to hospital network security.

Research Objectives

The focus of this research is to determine what the cybersecurity issues in the healthcare business are and how to reduce current security events in order to improve security in this profession. Current trends of security breaches in global healthcare networks should also be looked at. Finally, what more research can be done to improve healthcare safety?

Challengers In Healthcare Sector

Cyber-attacks on healthcare infrastructure, services, and medical equipment, which can compromise patient safety, are the most severe threat confronting the healthcare sector. Usability and accuracy are critical components of healthcare delivery, yet hackers are constantly on the lookout for vulnerable systems. The healthcare business attracts hackers because the sensitive data it contains is valuable and easy to get. The healthcare industry shares the majority of attack vectors with other businesses, but the consequences of a breach are even more serious because it involves human safety.

Priya and her colleagues Several health-care security assaults and threats involving the safety, integrity, and availability of private data. The authors divided security risks into three categories. Data collection, network collection, and storage A number of wireless gadgets are connected to the hospital's network. These Gadgets, on the other hand, assist physicians and other health workers in providing great patient care while simultaneously increasing the attack surface. [7] Ransomware is a sort of malware that encrypts a user's data in order to extort money. It is sometimes referred to as the "digital form of intimidation."

In recent years, ransomware has become one of the most widespread assaults against the healthcare industry. As mentioned in the introductory section, the WannaCry assault on the British National Health Service highlighted the impact of this sort of attack on critical infrastructure. Ransomware attackers frequently try to extort money from victims by encrypting files and causing data to be unavailable. [8] However, it is said that a recent ransomware assault on the podiatrist's office destroyed or altered 24,000 patient data.

In recent years, ransomware has become one of the most widespread assaults against the healthcare industry. As mentioned in the introductory section, the WannaCry assault on the British National Health Service highlighted the impact of this sort of attack on critical infrastructure. [9] Ransomware attackers frequently try to extort money from victims by encrypting files and causing data to be unavailable. However, it is said that a recent ransomware assault on the podiatrist's office destroyed or altered 24,000 patient data.

Attackers frequently use URLs to mislead unsuspecting victims into clicking on them, which then installs the Ransomware virus to their computers, but they also use techniques like drive-by shareware. Ransomware has become the preferred choice for hackers due to its ease of use, the availability of Ransomware toolkits, and decentralized currency such as Bitcoin. In the case of the National Health Service of the United Kingdom, WannaCry ransomware spread quickly from one system to another, infecting almost 50,000 workstations at its peak.

The subsections that follow go through some of the reasons why the healthcare sector is vulnerable to cyber-attacks. The most significant threat to the healthcare sector is an attack on the industry's infrastructure, services, and medical equipment, which can put patients' lives in jeopardy. Usability and accuracy are critical components of providing healthcare services, yet hackers are always on the lookout for vulnerable systems. Because of the significance of the sensitive data it carries and the simplicity of the aim, hackers are drawn to the healthcare industry.

The healthcare industry shares the majority of threat vectors with other industries, but the consequences of a breach are far more serious because it involves human safety. Priya et al. outlined some of the security threats aimed at healthcare systems, as well as the risks they pose to sensitive data security, integrity, and availability.

Emerging Trends in Cyber Security

Cyber-attacks can occur on any network connection or endpoint. The interoperability of software, operating systems, medical device

interfaces, and information exchange networks is a necessary condition for a digital healthcare system, and it is essential for network security risk management. The increasing physical traffic of medical networks, wireless connections, and the introduction of medical applications in healthcare have significantly expanded the attack surface and vectors. It is currently difficult to protect all access points of the health system. [10]

Medical Cyber Physical Systems

The Medical Internet of Things (MIoT) and implanted and wearable medical devices are referred to by this term. Hospitals are increasingly relying on cyber-physical medical systems (MCPS) to deliver high-quality care, and they've evolved into a platform for monitoring and treating a wide range of patient health issues. By 2020, link devices are expected to number 20 billion, and by 2028, they will number 50 billion. Because of its intrinsic qualities, the security issues associated with MCPS have grown. Because of these features, MCPS is more diverse, mobile, heterogeneous, and widespread. [11] [12]

They are typically left unattended (as with implanted devices) to collect sensitive physiological data, yet their size, power, and memory capacity are restricted, giving only minimal security capabilities. Because of the vulnerabilities of MCPS, its link to and dependency on the healthcare network substantially increases the cybersecurity risk to the whole healthcare system. For hostile actors, MCPS has become a key potential attack route, allowing for infiltration, malware installation, and treatment delivery manipulation.

Vulnerability scanning and patch management are examples of network security solutions that are either not accessible or can only be given by the manufacturer. There is a lack of clarity about MCPS aftermarket ownership, software upgrades, and security laws on a global scale. Manufacturers may be hesitant to disclose documentation that outlines device cybersecurity vulnerabilities or patch and update processes since this is considered proprietary information.

The lack of healthcare standards to enhance MCPS interoperability encourages incompatibility between various healthcare systems and medical devices56, resulting in a healthcare vendor market that rushes patient devices to market before cybersecurity issues are addressed. Please refer to the previous comment. Look over all of the notes. Medical device cybersecurity vulnerabilities, as well as a lack of vendor and regulatory monitoring, have been recognized as a strategic priority by the Australian Therapeutic Goods Administration. The lack of healthcare standards to enhance MCPS interoperability encourages incompatibility between various healthcare systems and medical devices, resulting in a healthcare vendor market that rushes patient devices to market before cybersecurity issues are addressed. Please refer to the previous comment. Look over all of the notes. Medical device cybersecurity vulnerabilities, as well as a lack of vendor and regulatory monitoring, have been recognized as a strategic priority by the Australian Therapeutic Goods Administration.

Data confidentiality, privacy, and consent

The second grant was the privacy and issue of the secret data of the patient around the usage of personal information. Cyber security may be classed as information concerning the danger of personal information on confidentiality, accessibility, and integrity. Confidentiality is harmful owing to personal health records or data loss, as well as consumer confidence. DENY (DOS) Malware or Ransomware assaults sacrifice health records, software platforms, operating systems, and access to hardware. The integrity of the data is harmful if the health data is distorted or deleted or interrupted to vital equipment and monitors. [13]

Because of its economic relevance and large attack surface, healthcare is both a sensitive and

tempting target for assault. 64 Given the importance of the health sector and the kind of user information kept inside health information systems, the health industry should place a higher focus on cybersecurity. Patients, healthcare providers, and identity thieves all place a high value on health information and medical data. Health data is believed to be ten to twenty times more valuable than credit card or banking information. If your credit card or bank information is stolen, you can update it. Health history or data that may be linked back to a single individual is not feasible.

Cloud Computing

Cloud computing has been identified as a data and information security concern during transit and storage. Because of the huge volume of health data collected, centralized data storage, encryption, deployment, and maintenance have become prohibitively expensive at the organizational level. Data storage, processing, and analysis may now be delegated to remote servers thanks to the advancement of cloud computing.

The attacker may get access to hypervisor processes and services (such as a virtual machine monitor, which is the computer software, firmware, or hardware that creates and operates virtual machines), as well as any application clients that may be utilized, if the host operating system has been compromised.

Health Application security

The combination of broad use in healthcare applications and a lack of security measures is viewed as posing a rising cybersecurity threat to personal data confidentiality and the integrity of the associated HCS infrastructure. Large quantities of personal health data may be generated, stored, and analyzed using health apps. WhatsApp is appealing for telemedicine because of its ubiquity, simplicity, low cost, and enhanced encryption, and it allows professional networking and team communication.

The health service promotes mental health as a viable, autonomous, and cost-effective alternative to face-to-face therapy. However, there is relatively little study on the safety of apps in medical practice, as well as the rise of authorized mental health and dementia applications. More than half of government-approved applications in Australia, according to a recent survey, lack a privacy policy that notifies users about how personal information will be collected, kept, and shared with others. Patients' confidentiality and safety, as well as communications security, are frequently overlooked by application developers, who are typically out of control in terms of content, authorship, and dependability. The health service promotes mental health as a viable, autonomous, and cost-effective alternative to face-to-face therapy. However, there is relatively little study on the safety of apps in medical practice, as well as the rise of authorized mental health and dementia applications. More than half of government-approved applications in Australia, according to a recent survey, lack a privacy policy that notifies users about how personal information will be collected, kept, and shared with others. Patients' confidentiality and safety, as well as communications security, are frequently overlooked by application developers, who are typically out of control in terms of content, authorship, and dependability.

Health applications can be vulnerable to both aggressive and passive assaults, resulting in data modification or theft, if adequate security measures are not in place.

Insider Threat

The combination of the pervasive usage of healthcare apps and the lack of security controls is viewed as a rising cybersecurity risk to the confidentiality of personal data and the integrity of the associated HCS infrastructure. Health applications may produce, store, and analyze enormous quantities of personal health data.

WhatsApp's ubiquity, simplicity, low cost, and increased encryption make it ideal for medical services under resource-limited situations and for encouraging professional networking and team collaboration.

The usage of WhatsApp among physicians is now so prevalent that urgent restrictions are needed to ensure that professionals do not unintentionally breach the privacy or confidentiality of patients. The health service emphasizes the use of mental health as an autonomous, accessible and lucrative alternative to face-to-face therapy. However, there is limited study on the safety of applications in medical practices and the rise of authorized applications for mental health and dementia. The use of WhatsApp among physicians is now quite popular and urgent restrictions are needed to guarantee that professionals do not unintentionally breach the privacy or confidentiality of the patient. The health service emphasizes the use of mental health as an autonomous, accessible and lucrative alternative to face-to-face therapy. However, there is relatively little study on the safety of apps in medical practice, as well as the rise of authorized mental health and dementia applications.

Network and Wireless Vulnerability

Web servers, databases, and application software are the most common targets of attacks that use the network as a carrier and attempt to exploit vulnerabilities in computers and devices connected to the network.

- **Database Servers**: Many devices and systems use databases or data stores to store information about the device. This is called the database backend. Many of these databases use structured query language (SQL), and if they are not properly configured to clean up the input data, they are extremely vulnerable to SQL injection attacks. SQL injection is a very dangerous threat because it destroys all three information security goals (confidentiality, integrity, and availability). The attacker can delete all information from the database, making it inaccessible. They can read all information, which violates confidentiality, and can inject fake data, which means loss of data integrity.

- **Web Servers**: Many devices and systems store information about themselves in databases or data storage. The database backend is what it's called. Many of these databases utilize structured query language (SQL), and thus are highly vulnerable to SQL injection attacks if they are not properly configured to clean up the input data. SQL injection is a particularly severe vulnerability because it undermines all three information security objectives (confidentiality, integrity, and availability). The attacker has the ability to erase all data from the database, rendering it unavailable. They have access to all information, which compromises confidentiality, and they can insert phoney data, jeopardizing data integrity.

- **Application Software:** This applies to any software that runs on the device, whether it's utilized in conjunction with the preceding two categories or on its own. The attack is more likely to succeed if the program has not been subjected to thorough software vulnerability testing to discover any potential weaknesses. Many successful cyberattacks have taken use of weaknesses in software that were not adequately vetted before being deployed in a live environment. [14]

The exploit technique might also be a direct assault, social engineering, malware, or a combination of these. Direct cyberattacks can happen when the user is relatively close to the

device and has a direct connection (wireless or physical), or when the user has a direct connection through a local or Internet network. Social engineering is the phase of an attack in which an attacker acquires information (such as passwords) from someone who understands the system or its security mechanisms via chat, email, or deceit.

Social engineering is used in the most effective attacks. The last group includes viruses, worms, Trojan horses, and sophisticated persistent threats. The application searches for and exploits known software flaws in order to take control of or damage the system. Traditionally, antivirus software has been employed to tackle this threat, but it has shown to be increasingly ineffectual.

Confidentiality, Integrity, and availability of Information

Due to weak access control mechanisms, unauthorized access (Confidentiality) may jeopardize confidentiality. The following are the consequences:

• Legal action and financial consequences,

• noncompliance with HIPAA [Health Insurance Portability and Accountability Act of 1996] requirements.

• reputational damage

Integrity can be jeopardized by poor configuration, data breaches, or illegal information modification. This will have an impact on:

• Patient safety from an attacker's use of the device

• Patient safety from potentially incorrect clinical judgments.

When access to data or a device is restricted or lost, availability occurs. The following are the consequences:

• When important notifications are not received, patient safety is jeopardized.

• Restricting access to critical information and influencing future therapeutic decisions endangers patient safety.

Most of the Critical Reasons for being vulnerable

Many factors influence medical device protection and keep the healthcare business in a dangerous situation. Technology, management, and human factors all play a role in this.

• Legacy operating systems and software (often devices, systems, and software that have been in use for more than 5 years or that have been replaced by newer versions) and system incompatibility, resulting in configuration mistakes and security risks. This includes flaws created by unnegotiated interfaces with third-party software, which are frequently accessible via web interfaces.

• Give hackers fundamental knowledge: certification organizations reveal device verification information, such as spectrum; radio frequency transmission data is included in equipment manuals; and patent databases include information on equipment operations. It is incorrect to rely on security in the dark, even if a proprietary protocol is used for communication. This not only limits interoperability, but it also leaves the door open to unprotected reverse engineering. Superior protection is

provided by the employment of robust, tried-and-true real-world network security technologies.

• Medical equipment is deficient in basic security precautions. Computed tomography scanners, for example, that give measured radiation, can be tampered with, creating a danger to patient safety. Security measures included during the design process, and occasionally during implementation, might disrupt clinical workflow if they are not handled properly.

• A lack of understanding of cybersecurity problems and poor security processes exacerbates the basic problem of uneven cybersecurity programs in device development and certification. Failure to securely dispose of devices containing information or data, password sharing, and password distribution, particularly in devices where passwords are required for device access, are all examples of poor practices. Inconsistent cybersecurity risk and consequence education and training also contributes to the persistence of cybersecurity vulnerabilities.

• Finding a balance between security and privacy concerns, as well as the utility and safety of health care, might be tough. Strong encryption and access control measures, for example, increase security but place the patient in more danger in the event of an emergency.

Cybersecurity Capability, countermeasures, and mitigation strategies.

Critical health information security and risk mitigation is becoming a global issue. The idea of a Cybersecurity Centre for Threat Control (based on the US Centers for Disease Control or a Cyber World Health Organization) is advocated to allow global recognition of the importance of international collaboration in combatting cybercrime. Data breach response plans should be included into organizational disaster plans, as well as proactive partnerships between governments, corporations, and healthcare providers, to improve and reinforce collective security across the healthcare sector.

- **Cryptographic Architecture or Technological Solution**

  To promote network security solutions, a lot of attention is devoted to technological solutions and sophisticated cryptography on a global scale. The majority of the records identified (n = 63) dealt with technological cybersecurity defensive designs, which were frequently created by the records' authors. The numerous encryption security solutions that may be utilized to handle the transmission of data and the storage of patient information through network systems, cloud settings, or remote patient monitoring devices are outside the scope of this paper. Two sorts of passwords will be briefly explained owing to their extensive relevance and potential assistance with health-related issues.

The second is blockchain. Blockchain is a peer-to-peer ledger system that began in the banking business. Due to its decentralization, verifiability, and immutability, blockchain can secure sensitive medical data. Immutability ensures that data on the blockchain cannot be altered or removed once it has been recorded. In terms of health, applications include the aggregation of research data and the integration of health information. All data on the blockchain is encrypted using public keys, including keywords and patient identities, and the keywords may be utilized for searches. Blockchain problems include scalability, security, and cost. [15]

- **Simulated Environments and Education**

  Employee cybersecurity education is the most important safeguard against data breaches, according to the newly released Australian papers. The importance of extensive staff training and education in order to recognize and assess risk is highlighted across the global records. Experienced managers, according to cybersecurity simulation models, make less effective cybersecurity decisions than novices because they are more likely to pursue an optimal option based on past experiences.

  Because of the unpredictable nature of 'zero-day' cyber-attacks and the ever-changing nature of cyber threats, making the best reactive judgments is sometimes hard. Rather, the ability to make proactive, preventative decisions is essential. Employees are frequently the unintended enablers of security breaches; as a result, behavioral skills training and education are required to increase privacy awareness and transform habitual information technology behaviors into conscious cybersecurity activities.

  Staff will take part in cybersecurity training if the interventions are not prohibitively expensive (i.e. time consuming or onerous) and if active engagement in the training promotes self-efficacy. Simulator-based training can help with this by allowing students to practice and improve their cybersecurity skills. It is impossible to overestimate the value of cybersecurity organizational capability and individual employee capabilities in reducing the risk of vulnerabilities and breaches.

  Employees will take part in cybersecurity training if the cost of the intervention is low (i.e., not time-consuming or expensive) and if actively participating in the training will increase self-efficacy. Through simulation-based training, this may assist develop and practice cybersecurity competencies. To decrease the risk of vulnerabilities and vulnerabilities, cybersecurity organizational capabilities and employee personal skills are critical.

- **Risk Assessment and governance**

  Healthcare data breaches are on the rise, with at least one breach in the health industry occurring every day throughout the world. A healthcare data breach cost an average of $6.45 million in 2019, up from $4.08 million in 2017–18. In any other industry, the average overall cost of a data breach is more than six times higher. On average, it takes the healthcare industry the longest to identify (mean 236 days) and remedy (93 days) a data breach. The greater the expected loss, the longer a breach goes undetected. It is impossible to overestimate the value of a thorough network security risk assessment in proactively finding

vulnerabilities and detecting assaults or system flaws. This should involve a complete assessment and analysis of the cybersecurity risks and sensitivity of all information technology hardware, software, and MCPS, as well as third-party vendor or partner cybersecurity policies. Healthcare cybersecurity risk assessments and plan frameworks should be harmonized across nations, and vendor cybersecurity compliance and responsibility standards should be included.

Best Practice Technical Controls

Various technological best practice methods may be implemented to avoid network security vulnerabilities. The issue, on the other hand, is how to safely incorporate controls inside complicated systems. Encryption and passwords, for example, are popular security techniques, and it's essential to figure out which medical equipment don't use them. Furthermore, although they are seldom utilized, proximity-based access control and distance limits may be acceptable remedies for vulnerabilities in remote access and insecure web interfaces.

In circumstances involving sensitive data, data leakage detection, prevention, and monitoring linked with information management systems might be beneficial. Although data leakage protection software is available, it requires considerable policy design and configuration on the part of the business. These kinds of solutions must be integrated into a wider business strategy and are not a panacea for all cybersecurity issues.

Conclusion

This study looks at studies on worldwide cyber-attacks in the healthcare industry in order to categorize cyber health hazards and offer mitigation countermeasures or security techniques for generic electronic health records. Cyberattacks on healthcare are on the rise as a result of the cost-effective patient data available in digital medical systems, as well as a lack of cybersecurity protections and healthcare knowledge. Another issue is the hospital industry's underinvestment in network security and the antiquated medical IT system. This study looks at studies on worldwide cyber-attacks in the healthcare industry in order to categorize cyber health hazards and offer mitigation countermeasures or security techniques for generic electronic health records. Cyber-attacks on healthcare are on the rise as a result of the cost-effective patient data available in digital medical systems, as well as a lack of cybersecurity protections and healthcare knowledge. Another issue is the hospital industry's underinvestment in network security and the antiquated medical IT system.

Health management training is lacking in cybersecurity information, and the health system will remain susceptible until this issue is rectified. It's debatable if healthcare executives can lead improvements in the development of workplace healthcare cybersecurity capabilities and flexibility if they don't master critical cybersecurity skills. The threat of cybersecurity events or harm to the healthcare system cannot be eliminated internationally or in Australia. Establishing a proactive health culture with cyber security maturity, on the other hand, can assist decrease cyber security threats. Health management training is lacking in cybersecurity information, and the health system will remain susceptible until this issue is rectified. It's debatable if healthcare managers can lead the growth and evolution of healthcare cybersecurity and resilience capabilities in the workplace if they don't master key cybersecurity skills. They will not be able to completely remove the risk of cybersecurity events or damage to the healthcare system, either worldwide or in Australia. Establishing an active health culture with cybersecurity maturity, on the other hand, can assist decrease cybersecurity threats.

Future Research

Data would be shared, collected, and analyzed carefully. This previously inaccessible knowledge will be used by health companies to improve organizational efficiency and boost customer interaction, resulting in new value. Companies must pay more attention to data privacy and take efforts to enhance data security standards while this transition occurs. They're under increasing pressure to improve their understanding of cyber security risks in healthcare, as well as their detection and response skills.

Acknowledgement

First and foremost, I'd want to express my gratitude to Mr. Kanishka Yepa, a professor at Sri Lanka's Informatics Institute, for his unwavering support throughout my studies, as well as his patience, commitment, excitement, and vast knowledge. His study and writing advice were really useful, and I could not have asked for a better instructor and mentor for my graduation.

I owe a huge debt of gratitude to my colleagues at the Sri Lankan Institute of Information Technology's cyber security team for inspiring me and assisting me in successfully completing this assignment.

Finally, I'd want to express my gratitude to my family for their spiritual support throughout my studies.

References

[1] E. Thomas, "Hack of Melbourne medical records shows," 22 February 2019.

[2] C. Blumer, "My Health Record agency adds reputation," *ABC Investigations*, 24 05 2018.

[3] "Victorian patient health data 'highly vulnerable' to attack, Auditor-General's hack finds," 30 05 2019.

[4] A. g. o. h. Victorian, vol. Abc.net.au, 30 05 2019.

[5] A. B. M. B. Abd-alrazaqa, T. Farraghera and P. , "Gardner, "Factors that Affect the Use of Electronic".

[6] N. S. Abouzakhar, *Internet of things security*, 14 02 2018.

[7] "G. Martin, P. Martin, C. Hankin, A. Darzi and J.," *Kinross, in Cybersecurity and healthcare: how safe are* , p. 358, 2017.

[8] S. S. P. R. a. S. R. Priya, "A survey on security attacks in electronic," no. 691-694, 2017.

[9] S. W.-F. A. f. Healthcare, *FORTINET*, 17 11 2017.

[10] D. &. Dumitrache, " Cyber Security in Healthcare," 2017.

[11] L. Cilliers, "Health Information Management Journal," *Wearable Devices in Healthcare Privacy* .

[12] S. Writers, "OPM hack linked to attack on US insurer Anthem," 2019.

[13] .. J. T. P. M. T. P.-J. B. K. Huckvale, "BMC Medicine," *Unaddressed privacy risks* , 2015.

[14] J. H. a. B. Irwin, "Testing antivirus engines to determine their effectiveness as a security layer," 2014.

[15] J. R. M. V. K. K. V. L. M. N. E. G. O. S. E. P. Natsiavas, "BMC Medical Informatics and Decision Making volume," 2018.

Author Profile

W.M J.P.Wijesekara was born in Bandarawela, Uva Province, Sri Lanka, in 1998. He is currently studying at the Sri Lanka Institute of Information Technology in Malabe. He went to Dharmapala Central college Bandarawela from secondary education. He learns BSc(Hons) in Information Technology Specializing in Cyber Security degree program.