Critical Infrastructure Security in the Healthcare Sector

Weerasiri H.A.K.D.(IT19154640)
Sri Lanka Institute of Information Technology

Abstract— The Internet of Things has produced a new generation of medical devices with enhanced sensing and actuation capabilities. To guarantee the sustained safety of patients, preventive mitigation of cyber threats that occur in this hyperconnected environment is required. Technology is increasingly integrated into the healthcare industry, thus improving the precision of medical care; however, progress still needs to be made in network security. However, advances in network security are still needed. According to a 2016 study by IBM and the Ponemon Institute, the frequency of data breaches in the healthcare business has increased since 2010 and is now one of the most hacked industries in the world. Criminals are particularly interested in the information obtained through health data breaches due to its immutability. An individual's medical file contains information such as blood type, previous operations and illnesses, and other personal health information. Because these records contain private data such as name, birth date, insurance, and health provider information, and also health and genetic material, restoring privacy or reversing psychological harm is impossible when personal information is breached. These kinds of cyberattacks not only harm patients' identities and finances but may also disrupt hospital operations and endanger patients' health and well-being. Because of the loss of access to hospital information systems caused by the WannaCry ransomware attacks in May 2017, hospitals in the United Kingdom's National Health System were forced to postpone treatment plans and even redirect arriving ambulances. Among the operational delays and financial implications of data breaches and ransomware attacks, cyberattacks have long-term negative impacts on hospitals' and health institutions' reputations and revenues.

IndexTerms- cybersecurity;cyberattack;cyberrisk;computer security;healthcare sector; risk management; electronic health records

INTRODUCTION

Health care is a basic need of humanity and affects all members of society. The healthcare business is responsible for acquiring and storing highly sensitive and confidential data while sharing this data with medical personnel, patients, and other organizations. The health system (HCS) is under pressure to maintain technological advancement. Digitization of health records helps the transition of healthcare from a hospital-centric, expert-centric approach to patient-centric distributed care, generally seen as inevitable and essential. [1] [2]

HCS network security breaches that expose sensitive information or data will be harmful to patients and medical institutions and may even lead to death. [3] Ransomware attacks, personal medical device hacking, and data theft increase the cyber security risks of healthcare. [4] Since personal data is very precious, hacked health data is more valuable than any other industry record. [5] [6]

They can be found on the dark web and can be used to fund crimes such as identity fraud, blackmail, blackmail, and even murder. For example, within a few months of 2015, both the US Office of Personnel Management (OPM) and Anthem Wellness, which provides healthcare services to government employees, were hacked by the same hacker. As a result, criminals will be able to link employment records with important health information of government employees, thereby enabling them to cause harm to high-value individuals. Despite the increase in cyber-attacks against healthcare organizations around the world, the healthcare industry often lags behind other companies in protecting critical information.

Although cybersecurity in healthcare has been identified as an increasingly serious health and safety issue, there is a lack of awareness of the dangers in the healthcare industry. To respond to the growing cyber threats, a strategy for healthcare cybersecurity capabilities needs to be developed. The recently launched Australian National Electronic Medical Record My Health Record (MHR) provides an opportunity to check the security capabilities of healthcare networks.

Increasing cyber security capabilities involve not only updating the current information infrastructure, but also proactively identifying and stimulating the need for new technologies, cyber security insights, and rigorous organizational training. The transition to digital healthcare requires the use of information technology to store large amounts of electronic patient data on various operating systems. Integrating new technologies with outdated, outdated, or unsupported operating systems can compromise interoperability and increase cybersecurity threats. The global WannaCry ransomware outbreak in 2017 is a good example.

Due to the widespread use of outdated Windows XP applications and the disdain to update the system's cybersecurity notifications, the malware spread in the UK's National Health Service (NHS). WannaCry was the largest ransomware outbreak to date, causing the NHS to be unable to provide patient care for a week between May 12-17, 2017, affecting 200,000 computers in more than 100 countries. Due

to inadequate cyber hygiene and lack of understanding of the business risk consequences of cyber intrusions by executive healthcare managers, WannaCry was able to expand to 80 out of 236 NHS trusts and 603 primary care organizations in England.

Ambulances were diverted, test equipment was contaminated, pathology and radiology were not working, patient records were inaccessible, and more than 7,000 medical appointments were canceled. Compared to other industries, healthcare is known for its low level of security expertise and the lack of modern data security measures. Budget constraints, lack of network security training and awareness among health managers, different health information systems, and a large number of connected wireless devices are all issues. Cyber defense in the healthcare sector is now mainly passive, and measures are only taken after a malicious attack occurs.

The traceability of health network security and the industry's reliance on perimeter defenses (antivirus, firewall) have exacerbated network risks. Complex and ongoing attacks and insider threats are unlikely to be solved by such protection measures. Another major obstacle to hospital network security is the lack of trained network security experts in the field, as well as evolving malware threats and complex network infrastructure.

Research Objectives

This research aims to study what are the cybersecurity problems in the healthcare industry and how to minimize current security incidents to improve security in this field. Additionally, current patterns of security breaches in global healthcare networks should be investigated. Finally, what more research can be done to improve safety in the healthcare sector

Challengers In Healthcare Sector

The most dangerous facing the healthcare industry is cyber-attacks on healthcare infrastructure, services, and medical equipment, which can jeopardize patient safety. Usability and accuracy are important aspects of healthcare delivery, but they are targeted by hackers who are always looking for systems with weak targets. Hackers are attracted to the healthcare industry because the sensitive data it contains is important and easy to use. The healthcare industry shares most threat vectors with other companies, but the consequences of compromise are much greater because it affects human safety. [7]

Priya et al. [8] Several security attacks for health systems and threats representing safety, integrity, and availability of confidential data. The authors categorized the threats of security in three phases. Data gathering, network gathering, and storage. There are several wireless devices connected to the hospital network. However, these Gadgets help provide physicians and other health workers with excellent patient care, but they also expand the attack surface. [9]

Ransomware is a type of virus type virus that encrypts the user's data to extract money and is often called the digital form of intimidation.

Ransomware is one of the most common attacks frequently used against the healthcare industry in recent years. The WannaCry incident that affected the British National Health Service demonstrated the impact of this type of attack on important infrastructure, as described in the introduction section above. Ransomware attackers often try to squeeze money from victims by encrypting files and disturbing the availability of data. However, a recent ransomware attack on the podiatrist's office is said to have damaged or changed 24,000 patient records. [10]

Attackers often trick unsuspecting victims by giving them URLs to click on, which subsequently downloads the Ransomware malware to their PCs, but they also employ tactics such as drive-by shareware. Because of its simplicity of usage, the availability of Ransomware toolkits, and decentralized cryptocurrencies such as Bitcoin, ransomware has become the favored alternative for hackers. In the instance of the United Kingdom's National Health Service, the WannaCry ransomware moved swiftly from one system to another, infecting nearly 50,000 workstations at its height. [11]

The following subsections discuss some of the reasons why the healthcare industry is vulnerable to cyber-attacks. The most serious threat facing the healthcare industry attacks healthcare infrastructure, services, and medical equipment, which can endanger the safety of patients. Usability and accuracy are important aspects of providing healthcare services, but they are being attacked by hackers constantly looking for weak systems. Hackers are attracted to the healthcare industry because of the importance of the confidential data it contains and the simplicity of the goal.

The healthcare industry shares most of the threat vectors with other businesses, but the consequence of a compromise is significantly greater because it affects human safety. Priya et al. highlighted some of the security assaults aimed at healthcare systems, as well as the threats they represent to the security, integrity, and availability of sensitive data.

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. [12]

- **Medical Cyber Physical Systems**
  The phrase refers to the Medical Internet of Things (MIoT) and implantable and wearable medical devices. Hospitals are increasingly using cyber-physical medical systems (MCPS) to provide high-quality treatment, and they have become a potential platform for monitoring and managing many aspects of patient health. It is estimated that by 2020, link devices will reach 20 billion and by 2028 they will reach 50 billion. [13] The security concerns inherent in MCPS are increased due to its inherent features. These characteristics make MCPS diversified, mobile, heterogeneous, and more common.

They are frequently left unattended (as with implanted devices) to capture sensitive physiological data and are limited in size, power, and memory capacity, providing only rudimentary security capabilities. Because MCPS characteristics render them vulnerable to compromise, its connection to and dependence on the healthcare network dramatically raises the cybersecurity risk to the whole healthcare system. MCPS has grown to be significant potential attack channels for hostile actors, allowing for penetration, malware installation, and treatment delivery modification. [14]

Network security methods, such as vulnerability scanning and patch management, are not available or can only be provided by the manufacturer. Internationally, there is a lack of clarity regarding MCPS aftermarket ownership, software updates, and security regulations. Because this is considered confidential information, manufacturers may be reluctant to release documentation that describes device cybersecurity vulnerabilities or patch and update procedures.

The lack of healthcare standards to encourage MCPS interoperability promotes incompatibility between various healthcare systems and medical devices, creating a healthcare vendor market that rushes patient devices to market before cybersecurity problems are addressed. Look through all the notes The Australian Therapeutic Goods Administration has identified medical device cybersecurity vulnerabilities, as well as a lack of vendor and regulatory monitoring, as a strategic priority. The lack of healthcare standards to encourage MCPS interoperability promotes incompatibility between various healthcare systems and medical devices, creating a healthcare vendor market that rushes patient devices to market before cybersecurity problems are addressed. Please see the preceding comment. Look through all the notes The Australian Therapeutic Goods Administration has identified medical device cybersecurity vulnerabilities, as well as a lack of vendor and regulatory monitoring, as a strategic priority. [15]

- **Cloud Computing**

  Cloud computing has been recognized as a network security issue for data and information during transportation and storage. Due to the large amount of health information generated, centralized data storage, encryption, deployment, and maintenance have become very expensive at the level of a single organization. With the development of cloud computing, it becomes possible to outsource data storage, processing, and analysis to remote servers. [16]. The hacked host operating system may allow the attacker to access hypervisor processes and services (such as a virtual machine monitor, which is the computer software, firmware, or hardware that builds and runs virtual machines), as well as any application clients that may be used. [17]

- **Health Application security**

  The combination of widespread use in healthcare applications and the lack of security safeguards is seen as a growing cybersecurity risk to the confidentiality of personal data and the integrity of the linked HCS infrastructure. Health applications can generate, store, and analyze large amounts of personal health data. WhatsApp's ubiquity, simplicity, low cost, and improved encryption make it attractive for telemedicine when resources are limited, and it supports professional networking and team communication.

  The health service promotes the application of mental health as an independent, accessible, and profitable alternative to face-to-face treatment. However, there is very little research on the safety of applications in medical practice and the growth of approved applications for mental health and dementia. A recent study in Australia found that more than half of government-approved apps lack a privacy policy that informs users of how personal information will be collected, stored, and shared with others. Application developers often overlook patient confidentiality and safety, as well as communications security, and are generally out of control in terms of content, authorship, or reliability. The health service promotes the application of mental health as an independent, accessible, and profitable alternative to face-to-face treatment. However, there is very little research on the safety of applications in medical practice and the growth of approved applications for mental health and dementia. A recent study in Australia found that more than half of government-approved apps lack a privacy policy that informs users of how personal information will be collected, stored, and shared with others. Application developers often overlook patient confidentiality and safety, as well as communications security, and are generally out of control in terms of content, authorship, or reliability.

  The authors of a cross-sectional survey on the privacy and information security of health apps on wearable devices [18] found that respondents (n = 106) did not know the confidentiality or security of data collected from their apps on wearable devices , including what was obtained and how it was transmitted or stored. The authors hypothesize that these findings indicate that the public lacks a broader understanding of potential data security and privacy issues. Worryingly, these apps have been approved by regulatory agencies for use by patients with dementia and mental illness.

  Health apps can be subject to both active and passive assaults, resulting in data alteration or theft, if sufficient security measures are not in place.

Data confidentiality, privacy, and consent

The second grant was the privacy and problem of the secret data of the patient surrounding the use of personal information. Cyber security can be classified as information about the risk of personal information on confidentiality, accessibility, and

integrity. Confidentiality is dangerous due to personal health records or data loss, as well as customer confidence. DENY (DOS) Malware or Ransomware attacks sacrifice health records, software platforms, operating systems, and access to hardware. The integrity of the data is dangerous if the health data is distorted or destroyed or interrupted to critical devices and monitors.

Because of its economic significance and vast attack surface, healthcare is both a susceptible and appealing target for assault. Given the importance of the health sector and the sort of user information held inside health information systems, the health sector should place a greater emphasis on cybersecurity. Patients, healthcare providers, and identity fraudsters all place a high value on health information and medical data. Health data is estimated to be ten to twenty times more valuable than credit card or banking information. If your credit card or financial information is stolen, you can update it. Health history or data that can be traced back to a specific individual is not possible. [19]

Insider Threat

The combination of the ubiquitous use of healthcare applications and the lack of security safeguards is seen as a growing cybersecurity risk to the confidentiality of personal data and the integrity of the linked HCS infrastructure. Health apps can generate, store, and analyze large amounts of personal health data. WhatsApp's ubiquity, simplicity, low cost, and enhanced encryption make it attractive for medical services under resource-limited conditions and for promoting professional networking and team communication.

The use of WhatsApp among doctors is now so common that urgent rules are needed to ensure that professionals do not accidentally invade the privacy or confidentiality of patients. The health service promotes the application of mental health as an independent, accessible and profitable alternative to face-to-face treatment. However, there is little research on the safety of applications in medical practice and the growth of approved applications for mental health and dementia. The use of WhatsApp among doctors is now very common and urgent rules are needed to ensure that professionals do not accidentally invade the privacy or confidentiality of the patient. The health service promotes the application of mental health as an independent, accessible and profitable alternative to face-to-face treatment. However, there is very little research on the safety of applications in medical practice and the growth of approved applications for mental health and dementia.

The author of a cross-sectional survey on the privacy and information security of health apps in wearable devices discovered a lack of awareness among respondents (n = 106) about the confidentiality or security of data collected from their wearable device apps, including what was obtained and how it was transmitted or stored. The author hypothesizes that these findings indicate a broader lack of awareness among the general populace regarding potential data security and privacy issues. It's concerning that the government has approved these applications for usage in people suffering from dementia and mental illness. [20]

Network and Wireless Vulnerability

Attacks that use the network as a carrier and attempt to attack vulnerabilities in computers and devices connected to the network usually target three targets: Web servers, databases, and application software.

- **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**: It is very common to use Web services to interact with medical devices and provide a graphical interface through which you can configure or communicate with the device. The disadvantage of using this interface is that online services usually have vulnerabilities that can be easily exploited by attackers. There are a variety of attack tools available for free download and use to scan the web interface and identify any vulnerabilities in online services. Attackers can use this information to create custom payloads to attack vulnerable targets.

- **Application Software:** This applies to any program running on the device, regardless of whether it is used in combination with the first two categories or alone. If the software has not undergone extensive software vulnerability testing to find out what flaws may exist, the attack is more likely to be successful. Many successful cyberattacks have exploited flaws in the code that have not been thoroughly tested before being deployed in a real-time environment. [21]

In addition to these categories, the exploit technology can also be a direct attack, social engineering, malware, or a combination of these. Direct attacks can occur through a direct connection (wireless or physical) to the device, where the user is very close to the device, or a direct connection can be created through a local or Internet network. The attack phase in which an attacker obtains information (such as passwords) from someone who knows the system or its security measures through chat, email, or deception is called social engineering.

The most effective attacks involve some form of social engineering. Viruses, worms, Trojan horses, and advanced persistent threats make up the last group. The program finds and uses known software vulnerabilities to control or damage the

machine. Antivirus software has traditionally been used to combat this danger, but it has proven increasingly ineffective.

Confidentiality, Integrity, and availability of Information

Unauthorized access(Confidentiality) may jeopardize confidentiality owing to weak access control mechanisms. The ramifications of this are as follows:

- Legal action and financial ramifications,
- noncompliance with requirements (HIPAA [Health Insurance Portability and Accountability Act of 1996]),
- reputational damage.

Weak configuration, data breaches, or illegal information modification can all compromise integrity. This will affect on:

- Patient safety from an attacker's use of the gadget,
- Patient safety from possibly erroneous clinical judgments.

Availability occurs when access to data or a device is restricted or lost. The ramifications of this are as follows:

- Patient safety is jeopardized when important notifications are not received.
- Patient safety is jeopardized as a result of restricting access to essential information and influencing future therapeutic decisions.

Most of the Critical Reasons for being vulnerable

Many reasons affect the protection of medical devices and cause the healthcare industry to remain in an unsafe state. These are the results of technology, management, and human factors.

- Legacy operating systems and software (usually devices, systems, and software that have been used for more than 5 years or have been replaced by new versions) and system incompatibility, leaving vulnerabilities such as configuration errors and security vulnerabilities. This includes vulnerabilities caused by interfaces not negotiated with third-party software, which are often accessed through web interfaces.

- Provide basic information to hackers: certification bodies disclose equipment verification information, such as spectrum; radio frequency transmission data is provided in equipment manuals, and equipment operations are available in patent databases. Even if a proprietary protocol is used for communication, it is wrong to rely on security in the dark. This not only limits interoperability but also opens the door to reverse engineering without protection. The use of powerful, tried-and-tested real network security methods provides superior protection.

- Basic security measures are lacking in medical equipment. For example, computed tomography scanners that provide measured radiation can be tampered with, possibly posing a risk to patient safety. Security measures added during the design phase, and occasionally during implementation, might interrupt clinical workflow and are badly implemented.

- The fundamental problem of inconsistent cybersecurity programs in device development and certification is exacerbated by a lack of knowledge of cybersecurity concerns and inadequate security procedures. Poor practices include the failure to securely dispose of devices carrying information or data, password sharing, and password dissemination, particularly in devices where passwords are required for device access. Inconsistent education and training on cybersecurity risks and consequences also contribute to the persistence of cybersecurity vulnerabilities.

- It might be difficult to strike a compromise between security and privacy requirements, as well as health care usefulness and safety. For example, while robust encryption and access control mechanisms improve security, they put the patient in more danger in the event of an emergency.

Cybersecurity Capability, countermeasures, and mitigation strategies.

The security and mitigation of risks to critical health information is becoming a global priority. To allow worldwide acknowledgment of the necessity for international collaboration in combating cybercrime, the notion of a Cybersecurity Centre for Threat Control (based on the US Centers for Disease Control or a Cyber World Health Organization) is proposed. It is recommended that data breach response plans be integrated into organizational catastrophe plans, as well as proactive collaborations between governments, businesses, and providers to improve and strengthen collective security across healthcare sectors.

- **Cryptographic Architecture or Technological Solution**
  Internationally, great attention is paid to technical solutions and advanced cryptography to promote network security solutions. Most of the records found (n = 63) involved technical cybersecurity defense architectures, which were often built by the authors of the records. It is beyond the scope of this article to evaluate and explain the many encryption security options that can be used to address the exchange of data and the storage of patient information through network systems, cloud configurations, or patient monitoring devices remote. However, due to their wide relevance and possible help for health-related

problems, two types of passwords will be briefly described.

Blockchain is the second. Blockchain is a peer-to-peer ledger technology that was first used in the banking industry. Blockchain can protect sensitive medical information due to its decentralization, verifiability, and immutability. Immutability ensures that once data is recorded on the blockchain, it cannot be changed or deleted. In terms of health, applications include the integration of health information and the aggregation of research data. On the blockchain, all data, including keywords and patient identities, is encrypted with public keys, and the keywords can be used for searches. Scalability, security, and cost are all blockchain issues. [22]

- **Simulated Environments and Education**
  The revealed Australian documents do not address the fact that employee cybersecurity education is the most essential measure against data breaches. Throughout the worldwide records, the critical necessity for thorough staff training and education to allow risk detection and assessment is emphasized. According to cybersecurity simulation models, experienced managers make less effective cybersecurity judgments than novices because they are more prone to seek an ideal decision based on prior experiences.

  Because of the unexpected nature of 'zero-day' cyber-attacks and the ever-changing nature of cyber threats, optimum reactionary decisions are frequently impossible. Instead, the capacity to make proactive preventative judgments is critical. Employees are frequently the unintentional enablers of security breaches; therefore, behavioral skills training and education to improve privacy-protection awareness and convert habitual information technology behaviors into conscious cybersecurity actions are necessary.

  Staff will participate in cybersecurity provided interventions are not costly (i.e. time demanding or onerous) and if active participation in the training increases self-efficacy. This can be aided through simulation-based training to practice and build cybersecurity competencies. The importance of cybersecurity organizational capacity and individual employee skills in mitigating the risk of vulnerabilities and breaches cannot be overstated.

  Employees will participate in cybersecurity, as long as the cost of the intervention is not high (that is, time-consuming or expensive), and if actively participating in training can improve self-efficacy. This can help practice and develop cybersecurity capabilities through simulation-based training. The importance of cybersecurity organizational capabilities and employee personal skills to reduce the risk of vulnerabilities and vulnerabilities cannot be overemphasized.

- **Risk Assessment and governance**
  Healthcare data breaches are on the rise, with at least one breach occurring every day in the health business worldwide. The average overall cost of a healthcare data breach in 2019 was $6.45 million, up from $4.08 million in 2017–18. This is more than six times the average overall cost of a data breach in any other industry. The healthcare business takes the longest on average to detect (mean 236 days) and correct (93 days) a data breach. The bigger the anticipated cost, the longer a breach remains undiscovered.

The importance of a thorough network security risk assessment for proactively identifying vulnerabilities and detecting attacks or system vulnerabilities cannot be underestimated. This should include a thorough evaluation and analysis of the cybersecurity risks and sensitivities of all information technology hardware, software, and MCPS, as well as the cybersecurity protocols of third-party vendors or partners. Healthcare cybersecurity risk assessments and plan frameworks should be standardized across countries and include requirements for vendor cybersecurity compliance and responsibility.

Best Practice Technical Controls

To avoid network security vulnerabilities, various technical best practice measures can be used. However, the problem lies in the safe implementation of controls within complex systems. For example, encryption and passwords are common security methods and it is critical to determine which medical devices are not using them. Additionally, proximity-based access control and distance restrictions may be appropriate solutions for weaknesses in remote access and insecure web interfaces, although they are rarely used.

Data leakage detection, prevention, and monitoring integrated with information management systems can be useful in situations involving sensitive information. Although software for data leakage protection is available, it is dependent on extensive organizational policy formulation and configuration. Such solutions must be part of a larger corporate solution and are not a panacea for all cybersecurity concerns.

Conclusion

This review examines research data on global cyber-attacks in the healthcare sector to classify cyber health risks and provide mitigation countermeasures or protection methods related to general electronic health records. Due to the cost-effective patient data available in digital medical systems, as well as a lack of cybersecurity defenses and healthcare awareness, cyberattacks on healthcare are on the rise. Another problem is the outdated medical IT system and the hospital industry's underinvestment in network security. This review examines research data on global cyber-attacks in the healthcare sector to classify cyber health risks and provide mitigation countermeasures or protection methods related to general electronic health records. Due to the cost-effective patient data available in digital medical systems, as well as a lack of cybersecurity defenses and healthcare awareness, cyberattacks

on healthcare are on the rise. Another problem is the outdated medical IT system and the hospital industry's underinvestment in network security.

Health management training lacks information on cybersecurity, and until it is resolved, the health system will remain vulnerable. If healthcare managers do not learn key cybersecurity skills, it is questionable whether they can lead changes in the development of workplace healthcare cybersecurity capabilities and flexibility. Neither globally nor in Australia can eliminate the danger of cybersecurity incidents or damage to the healthcare system. On the other hand, establishing a proactive health culture with cyber security maturity can help reduce cyber security risks. Health management training lacks information on cybersecurity, and until it is resolved, the health system will remain vulnerable. If healthcare managers don't learn critical cybersecurity skills, it is questionable whether they can lead the development and change of healthcare cybersecurity and resilience capabilities in the workplace. Neither globally nor in Australia can they eliminate the danger of cybersecurity incidents or damage to the healthcare system. On the other hand, establishing an active health culture with maturity in cybersecurity can help reduce cybersecurity risks.

Future Research

Data would be shared, acquired, and thoroughly evaluated. Health organizations will leverage this previously unavailable intelligence to enhance organizational efficiency and increase customer contact, generating a new value. While this shift takes place, companies must pay greater attention to data privacy and take steps to upgrade data security requirements. They are now under growing pressure to have a better knowledge of cyber security threats in healthcare, as well as detection and response capabilities.

I. References

[1] Abc.net.au, "Hack of Melbourne medical records shows risk to health data," 22 February 2019. [Online]. Available: https://www.abc.net.au/news/2019-02-22/melbourne-heart-hack-cyber-criminals-my-health-record-risks/10834482.

[2] Abc.net.au, "My Health Record agency adds 'reputation', 'public interest' cancellation options to app contracts," 24 July 2018. [Online]. Available: https://www.abc.net.au/news/2018-07-24/digital-health-agency-changes-my-health-record-app-contracts/10026644.

[3] Abc.net.au, "A government office hacked Victorian hospitals. Here's what it found," 30 May 2019. [Online]. Available: https://www.abc.net.au/news/2019-05-30/victorian-hospitals-vulnerable-attack-auditor-general-hack-finds/11162352.

[4] Abd-alrazaqa , A., B. M. Bewicka; T. Farraghera; , P. Gardner, "Factors that Affect the Use of Electronic Personal," *international Journal of Medical Informatics 126 (2019)*, pp. 164-175, June 2019.

[5] N. S. Abouzakhar, A. Jones and O. Angelopoulou, "Internet of things security: A review of risks and threats to healthcare sector".

[6] Abrar, S. J. H. J. C. K. S. M. A. O. J.-M. and C. V. , "Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry," 14 February 2018.

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

[8] R. Priya, S. Sivasankaran, P. Ravisasthiri and S. Sivachandiran, *A survey on security attacks in electronic healthcare systems*, pp. 691-694, 2017.

[9] "Securing Wi-Fi Access for Healthcare," FORTINET, 17 November 2017. [Online]. Available: https://www.fortinet.com/blog/industry-trends/securing-wi-fi-access-for-healthcare.

[10] J. Davis, "Ransomware Corrupts 24,000 Patient Records of California Specialist," Xtelligent Healthcare Media, 07 January 2019. [Online]. Available: https://healthitsecurity.com/news/ransomware-corrupts-24000-patient-records-of-california-specialist.

[11] N. S. P. Traynor and K. Butler, "Making sense of the ransomware mess (and planning a sensible path forward)," vol. 36, no. IEEE Potentials, pp. 28-31, 2017.

[12] "Dogaru & Dumitrache, Cyber Security in Healthcare Networks.," 2017.

[13] L. Cilliers, "Health Information Management Journal," *Wearable Devices in Healthcare: Privacy and Information Security Issues.*

[14] A. Dubovitskaya, Z. Xu, . S. Ryu and M. Schumacher, "Proceedings - Annual Symposium proceedings.," *Secure and Trustable Electronic Medical Records Sharing using Blockchain*, pp. 650-659, 2017.

[15] M. Gaynor, T. Omer and J. S. Turner, "Journal of Healthcare Protection Management," *Teaching EHRs security with simulation for non-technical healthcare professionals*, vol. No 1, pp. 84-97, 2016.

[16] "Voluntary Data Breach Notification," IPC, [Online]. Available: https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification.

[17] "OPM hack linked to attack on US insurer Anthem," itnews, 201*9. [Online]. Available: https://www.itnews.com.au/news/opm-hack-linked-to-attack-on-us-insurer-anthem-405514.

[18] C. R. MacIntyre, T. E. Engells, . M. Scotch, . D. J. Heslop, A. B. Gumel, G. Poste, X. Chen, W. Herche, K. Steinhöfel, S. Lim and A. Broom , "Environment and System Decisions," *Converging and emerging threats to health security*, pp. 198-207, 2018.

[19] K. Huckvale, . J. T. Prieto, M. Tilney, P.-J. Benghozi and J. Car, "BMC Medicine," *Unaddressed privacy risks*

in accredited health and wellness apps: a cross-sectional systematic assessment, 2015.

[20] C. Morris, R. E. Scott and M. Mars, "Studies in Health Technology & Informatics," *Security and Other Ethical Concerns of Instant Messaging in Healtcare,* pp. 77-85, 2018.

[21] J. Haffejee and B. Irwin, *Testing antivirus engines to determine their effectiveness as a security layer,* no. IEEE, 2014.

[22] P. Natsiavas, J. Rasmussen, M. V. Knude, K. Votis,, L. Coppolino, . P. Campegiani, I. Cano, D. Marí, G. Faiella, . F. Clemente, M. Nalin, E. Grivas, O. Stan, E. Gelenbe and J. Dumortier, "BMC Medical Informatics and Decision Making volume," *Comprehensive user requirements engineering methodology for secure and interoperable health data exchange,* 2018.

Author Profile

H.A.K. Dakshina Weerasiri is an undergraduate in Sri Lanka Institute of Information Technology. He did Advanced Level at Panadura St.Jhons College and lives in Kalutara.