CYBRER SECURITY THREATS AND MITIGATIONS IN THE HEALTHCARE SECTOR: A LITERATURE REVIEW

IT20059422 WICKRAMASINGHE W A N
Department of Computer Systems Engineering Sri Lanka Institute of Information Technology
New Kandy Road Malabe 10115 Sri Lanka
It20059422@my.sliit.lk

I. ABSTRACT

More accurate healthcare is being provided because of greater use of technology, although improvements in cybersecurity are still needed. When it comes to data breaches, the healthcare business has seen a significant increase since 2010 [1]. In fact, it has become one of the most often targeted by cyberattacks worldwide [2]. The immutability of health data appeals to criminals especially [3]. A person's medical record contains a variety of health-related data, such as their blood type, previous procedures and diagnoses, and so on. For confidential records, such as those of a person's name, date of birth, insurance and health provider information, and health and genetic information to be restored or undone, it is very difficult.

Patients' personal information and financial resources are at risk, and hospital operations are hampered, putting the health and safety of patients in jeopardy. Hospitals in the United Kingdom's National Health Service were forced to postpone treatment plans and even reroute incoming ambulances after the WannaCry ransomware attacks in May 2017. In addition to the operational delays and financial expenditures associated with data breaches and ransomware attacks, cyberattacks have a long-term negative effect on hospitals' and health institutions' reputation and revenue.

Previously unprotected medical equipment is increasingly subject to cybersecurity risks because of greater access to existing computer networks. To avoid cybersecurity incidents, it is essential to understand the operational environment's complexity and catalog technical vulnerabilities. Cybersecurity protection is a more complex and complicated issue than it is a simple technical problem. There must be a thorough investigation of the components that make up this potentially dangerous environment and how these flaws might be exploited in order to find a remedy. When it comes to ensuring the safety and protection of patients, a comprehensive approach is needed. Technical controls, governance, resilience measures, standardized reporting, domain knowledge as well as legislation and regulations are required to achieve this end goal. It is self-evident that a determined, proactive strategy is required to deal with this difficult problem. In the meanwhile, there is a danger to the health of the patients. [3]

INDEX TERMS - cybersecurity, security, safety, wireless, risk, medical devices

II. INTRODUCTION

Technology advancements have the potential and power to improve patient outcomes via changes in the delivery of health care. The expanding interconnectedness of medical equipment and other healthcare systems is a notable illustration of this. Like other networked devices, medical equipment may be hacked due to its interconnectedness. In contrast to other types of networked computer systems, medical devices are increasingly worried about the impact they may have on clinical treatment and patient safety.

As networking, software, and operating systems all work together, the relative isolation and safety of medical equipment is more crucial than ever. Increasing complexity and administrative constraints reduce the capacity to defend. These problems are referred regarded as "cybersecurity vulnerabilities" in the industry lingo. Under the umbrella phrase "cybersecurity," there are a wide range of problems that are relevant to a given situation. "Cybersecurity" protects computer networks and their data against cyberattacks and intentional damage or interruption. 2 Management and security issues are just part of the challenge in the integration of medical devices, networks and software. When medical equipment is needed to be safety checked, there are a number of previously addressed problems. [4]

A recent SANS Institute survey found that 94% of healthcare firms had been attacked by cyberattacks, which are becoming more common in the sector. Attacks against critical infrastructure, such as hospitals and healthcare facilities, are covered in this category. 3 Regulators such as the FDA are responsible for ensuring that medical devices are safe, effective, and secure (FDA). Thus, regulatory agencies have issued recommendations to device manufacturers on how to handle cybersecurity risks and secure patient health information when submitting FDA-approved medical device applications. 4 Even though the recommendations stated here are merely suggestions, this shift in medical devices' working environments need immediate attention, even if they are only suggestions. Consequently, there's a lot of disagreement about what constitutes a medical device and what criteria should be used to classify software as one. To address these issues, new standards and updates to old ones have been developed and implemented by the standards community throughout the globe. Interoperability allows for the creation of innovative new types of health care while also enhancing patient safety. Medical device integration has been limited therefore, which might cause communication problems in the future. To ensure security, compatibility is not enough. [5]

Security authorities, hospital administrators, suppliers and manufacturers as well as scholars in the subject would benefit from this report's summation of the most relevant findings and recommendations from this working group. Our first step is to review some instances of health organizations' responses to similar assaults in the past. Afterwards, we'll go out for a drink. An approach to cybersecurity that emphasizes high-quality information technology, strong application foundations, and a resilient IT infrastructure is essential, as is an approach that is both

Confidence in the definition of medical devices has risen steadily over the last four years as a result of the FDA's finding that "software, electronic and electrical hardware, including wireless" that claims to be beneficial for medical reasons is covered by the Medical Device Data System Rule.

6 This definition is problematic since it includes data storage and data transportation, which are not priority for medical device makers in terms of data security. Maybe the requirement for interoperability has created more of a problem in terms of ancillary cybersecurity concerns than it has been possible to regulate for improved healthcare decision-making. Some of these flaws, which are not limited to the hardware or the connection, may be caused by technical hazards, software difficulties, or human factors of any combination. [5]

This article focuses on identifying attack paths and vulnerabilities, which is a complicated topic. [6] Consider the possible consequences of a security breach in order to understand how these vulnerabilities evolve on a systemic level. Medical device installation is just one part of the study's emphasis; it also examines the whole ecosystem in terms of cybersecurity issues. When it comes to a topic like this, generic information can't be avoided. cybersecurity. Thus, a multi-dimensional solution space is offered, together with its inherent difficulties. At the study's conclusion, the authors explore potential influences on medical device cybersecurity in the future. [7]

III. RESEARCH OBJECTIVE

proactive and preventive in nature. In a risk-based strategy, the identification of potentially sensitive IT assets is the first step. After then, it's a matter of finding the right mix of risk and reward. The scenario has both good and bad features. Security measures such as end-user education, vulnerability and patch management, restricted administrator rights, incident response and business continuity planning are all highlighted in this paper. Communication between the two sides is possible. Resilience can only be achieved if all stakeholders are included. Final ideas on ethical business methods that respect individual privacy will be offered. The transmission of data and the unique challenges presented by medical equipment pose a danger to security. [8]

IV. REVIEW OF THE LITERATURE

IV.I Case examples

The following examples of cybersecurity breaches demonstrate the breadth of assaults on the healthcare sector in many regions of the world, the implications of these attacks, and the efforts taken in response.

IV.I.I. ***.*** *ukaskrankenhaus Neuss (Germany)*

Neuss, Germany's Lukaskrankenhaus Neuss was established in 1911 and is a public hospital. It has a total of 1400 personnel and 537 bedrooms. A ransomware attack launched through social engineering in February 2016 resulted in a variety of error messages being displayed to employees. When a computer or server was hacked, the hospital took down its servers and computer systems to conduct a thorough examination and disinfection. Personnel used pen and paper and fax machines to continue working, although high-risk processes had to be delayed [15]. Despite not receiving a request for money directly, the hospital was given an email address to contact for further information. In accordance with the advice of local authorities, no attempt was made to contact the assailants [15].

As a result, although the hospital claims that just a few hours of data were lost due to an outage, there is still a backlog of handwritten notes that will need to be integrated into the EHR [15]. The hospital's spokeswoman predicted that it would be many months before the hospital's workflow returned to normal.

There was no evidence that patient data had been compromised.

IV.I.II. South-eastern Norway regional health authority (Norway)

As a state-run regional health authority, the Regional Health Authority of South-East Norway (South-East RHF) was founded in 2002 in partnership with three other regional authorities. The PHI and data of about 2.9 million people (more than half of Norway's population) were hacked by the South-East RHF in January 2018 [17]. A sophisticated criminal cell affiliated to a foreign espionage or state agency is likely to have carried out the attack, which targeted both patient health data and the health service's ties to Norway's military forces [18]. Older versions of Windows XP are thought to be to blame for the flaw. While the company was aiming to phase out Windows XP, the attack happened before the security measures could be deployed.

Concerns about future assaults on health data for political gain were raised by this assault, which did not appear to affect patient safety or hospital operations. By law, the company had to inform everyone impacted within 72 hours, but it failed to do so [20].

IV.I.III. ancock regional hospital (United States)

It was in 1951 when the Hancock Regional Hospital in Greenfield opened. SamSam [21], a ransomware, infected Hancock Regional on January 11th of this year. The attack targeted a server in the hospital's emergency IT backup system and spread via the electronic link between the backup location and the server farm there [22]. With the exception of backup files for electronic medical records, the hackers had destroyed all backup data. Researchers determined that the hackers exploited Microsoft's Remote Desktop Protocol and a hardware manufacturer administrator account to gain control of the server [22].

Following the attack, all networks and desktops were taken offline. However, hospital operations continued as normal. Nothing was done in terms of moving patients or shutting down the facility. The hackers had demanded a ransom of four Bitcoins (55,000 USD). After three and a half days of decryption, we were able to get the system operating again. In their investigation, they found no signs of a data breach. In an essay he published to explain his decision to pay the ransom, CEO Steve Long claimed that a sophisticated criminal organization had targeted the healthcare facility [22].

At the absolute least, a good application foundation and IT infrastructure are required for a health institution to have a sound information security posture. Because of the scarcity of personnel, financial restrictions, and a history of underinvestment, this is especially difficult in healthcare facilities, but it is an absolute necessity. The quality of a health care facility's information technology can't be evaluated using any formal models or methodologies. The problem may be clarified based on a few signs that have been spotted. There are no overwhelmed helpdesk call logs with break/fix requests at such a health institution, and its IT staff is not preoccupied with the restoration of faulty or damaged systems applications. [9]

The state of the IT infrastructure is also a factor in the quality of the IT services provided. A resource or service used to provide and support information technology services is referred to as "infrastructure" in this context (e.g., hardware platforms, software applications, operating systems, and networking and communications tools). Configuration, modification, and monitoring of IT infrastructure are all required for information security. IT assets and their interrelationships are tracked via configuration management. It is a requirement of the ITIL framework [11] to identify and report on the version of each asset as well as any connected elements. Although configuration management is time-consuming, it has a significant influence on vulnerability and patch management. Security, performance, accounting and fault management are all based on configuration management, according to SANS Institute. ITIL defines change management as a rigorous approach to standardize change management. Configuration management with change management is referred to as this by ITIL. A cyberattack is only one example of a circumstance where change management might be beneficial. One of the most basic forms of change management is an incident response plan. When it comes to promptly detecting and gathering information regarding assaults, IT departments rely heavily on audit logs and log data monitoring. [28] mentality that is proactive and careful. Consecutive Microsoft Windows upgrades often cause hospital equipment to reject or become functionally degraded. Patching operating system security issues has been put on hold or halted at several hospitals, therefore. Medical device makers are being urged to see cybersecurity as an asset and sell it as such as a result of a new value proposition for the industry. '12, 13" Rather than a nice-to-have, cybersecurity is becoming an absolute must in today's environment. After a product is on the market, the FDA requires manufacturers to keep up with on-going safety checks as part of their lifecycle operations [8]. The FDA implemented this rule in 2017 and requires medical device makers to show that their gadgets can be updated and patched throughout their useful lives. That's why it's so important for them to show that any possible patient damage from a compromised device has been dealt with. The FDA has the requirement to furnish a "bill of materials" to medical device purchasers. An item's provenance may be traced back to its source using the bill of materials. There are new requirements for manufacturers who are required by law to submit a 510(k)-premarket submission package. [13]

However, manufacturers bear the weight of these restrictions, health care facilities should also be forced to play an active part in defending themselves from cyberattacks. If hospitals have a long history of underinvesting in their staff, it may be difficult for them to engage in preemptive measures like allocating resources and planning early on.

Risk-based approach

Extreme steps are required when it comes to cybersecurity. Since there is no such thing as perfect cybersecurity, an enterprise risk management plan is required. Even if your IT infrastructure and procedures are of the greatest quality, you have a proactive mentality, and you have sufficient information security measures in place, you cannot completely remove the possibility of an attack. As a result, the internet security architecture recommended by the US National Institute of Standards and Technology (NIST) A risk-based strategy is, for example, used by the National Institute of Standards and Technology (NIST) and the European Union Agency for Network and Information Security (ENISA).

Vulnerability management is an important part of the NIST Cybersecurity Framework (CSF) for critical infrastructure since it helps to identify IT assets that are vulnerable to attack. It's important to prioritize asset protection based on the value and risk exposure of each asset.

This process of identification is strongly reliant on IT quality, particularly configuration management. The risk analysis of these outcomes should take into account the trade-offs between risks and rewards, as well as additional dangers [14].

Patients' safety and operation maintenance should also be taken into consideration. In the aftermath of an event, data and privacy protection (confidentiality), information availability, and information integrity must all be reviewed to establish the incident's effect. To ensure the safety of patients, it is critical to maintain the integrity of their medical records.

There are several methods in which health care institutions might lessen, decrease, or transfer risk [16]. The NIST CSF's following phases are Protect, Detect, Respond, and Recover [16].

To correctly identify, analyze, and manage information technology risks, several actions must be followed. But it also includes all the identifying steps: risk assessment, remediation or mitigation, and a reevaluation of the threat. Healthcare facilities should have an EDR system to monitor and analyze assaults and post-infection clean-ups. In most circumstances, this sort of risk assessment is almost impossible to do. If a health institution must operate around the clock, seven days a week, then the repair and mitigation procedures, such patch management, may be more difficult. administration of patches An organization's vital services and assets must be balanced against the sensitivity of server data during patching.

Companies should utilize penetration testing to find and repair holes in their systems. If a security vulnerability is discovered early, the chances of it spreading are greatly decreased. If a vulnerability has been discovered, it should be followed by the deployment of processes that do not put an overwhelming focus on zero-day vulnerabilities. According to Gartner analysts, most exploits are based on vulnerabilities that have been known to security and IT specialists for more than six months. These results should be taken into consideration when determining where to focus remedial efforts.

Configuration management helps in maintaining a high-quality IT infrastructure by making it easier to detect risks and do the analysis necessary for patching. Essential: Patchwork is a must.

Argaw et al. published their findings in BMC Medical Informatics and Decision Making (2020) 20:146. Page 5 of 10 should document any changes to the settings, such as updates to the operating system or third-party apps (including changes to the setting itself).

V. FUTURE RESEARCH

As a follow-up to the review, Now addresses possible options for further study in this area. According to prior studies, future study should include expanding or re-running existing studies (Zhou and colleagues, for example, 2018).

It's important to look at frameworks (e.g., Quaini et al. 2018) and design focused treatment solutions (e.g. Mamoshina et al., 2018). The following suggestions may be broken down into three general groups

the first group focuses on prospective technological advancements, while the second aims to enhance, medical services, and a growing need for more accurate data protection.

V.I. Inventions in the field of technology

Existing studies highlighted the need of concentrating on by focusing on technical concerns that might improve the performance of previously built frameworks

their real use within a medical environment Therefore, It is possible for researchers to focus their attention on concerns like strategic planning. management of nodes, automated generation or generation uploading of data and process improvement (Shen et al., 2019) Regarding the effectiveness of the system (Lee & Yang, 2018; Fan et al., 2018). To further enhance the scalability (Zhang et al., 2016) and functionality (Wong et al., 2019), academics have recommended for the extension of the present framework by considering fresh blockchain platforms in the construction of frameworks, for example (Rahmadika & Rhee, 2019). As a result, several academics have advocated for a more nuanced approach to the subject. current technology and algorithmic development for facilitating the development of more efficient blockchain-based healthcare networks. To this purpose, future academics may look at difficulties such as eliminating the requirement for worldwide smart contracts (Dagher et al., 2018), in conjunction with keyword searches (Zhang & Lin, 2018), There has been an increase in the amount of data that can be sent across systems.

V.II. Enhancing medical diagnostics.

Although there are algorithms for the implementation of blockchains, they are not widely used.

Despite efforts to improve healthcare, few studies have called on researchers to pay attention to the intricacies via means of bettering medical diagnosis (Mamoshina et al., 2018) and broadening their applicability beyond the realm of medicine to include rehabilitative treatment (Zheng et al., 2019). This is possible by way of improvements to testing procedures and diagnostic tools Dhagarra et al., 2018), remedial therapies for certain disorders 2019), as well as choosing which service providers should have preferential access to Medical documents in the event of an emergency (Brogan et al., 2018). Data security and privacy are top priorities for us.

There is a pressing need to improve current standards, according to existing research. data protection for ethical and legal use of medical data. Scholars need to concentrate on two important topics. " The first thing to consider is the future. compliance with the safety and regulatory requirements of research must be improved steps by addressing concerns such as ensuring the safety of employees and resolving vulnerabilities in the system with the purpose of enhancing robustness (Firdaus et al., 2018). Second, it is necessary to enhance the security and privacy of user data by to deal with challenges related to shared storage involves the release of keys (Al Omar et al., 2019). [18] [19]

VI. CONCLUSION

For the next year and a half after this conference, at least one hospital assault is recorded every other day. As of the beginning of October, ransomware has infected three institutions in Alabama (US), resulting in the evacuation of fresh patients. At the same time, ransomware was discovered in seven different hospitals throughout Australia. More of these assaults continue to take place, underscoring how severe this issue has become.

The cyber resilience of a hospital is a shared responsibility that must be given top priority. Healthcare workers (clinical and administrative) must get cybersecurity training and practice good digital hygiene, and politicians must put in place appropriate protocols and consider cybersecurity when making procurement decisions. This is critical.

Hospital information security teams should put in place and implement all necessary safeguards for the benefit of the facility and its patients.

Email filtering, URL scanning, whitelisting trusted websites and applications, and blocking of untrusted Flash and Java on the Internet should be provided by IT security teams in order to protect users against social engineering attacks. Another strategy to minimize risk is to regularly [20] change default passwords and refresh security settings on laptops, servers, workstations, and firewalls. In order to protect your data, penetration testing, limited physical access, and frequent backup upgrades all play a part (which should be stored offline). Website and industrial control systems like HVAC, security cameras, and fire alarm panels should be protected with appropriate security methods. It is possible to use EDR software to detect and respond to malware intrusions. In order to reduce the risk of security breaches, data should be transmitted between departments or medical institutions with privacy in mind.

Another major challenge is resolving the trade-offs associated with cybersecurity. [21]. Precision medicine requires careful consideration of security, privacy, and regulatory compliance, especially in distant and collaborative environments. However, convenience cannot be ignored. In the absence of this consideration, any advice will merely be theoretical. Rather than putting themselves at danger from cyber-threats, doctors are doing it for the sake of their patients' comfort and convenience, as well as an attempt to enhance the standard of care they provide. Medical personnel aren't irritated by security agents shutting down systems to install updates or patches, but rather, they're doing it to lessen the risk of disruption due to mass assaults. Instead of two separate factions, an interdisciplinary team should work together to ensure and enhance patient care and data security.. [22]

VII. ACKNOWLEDGEMENT

Would like to thank our Senior lecturer, Mr. Kanishka Yapa and the co-lecturer Miss P A C Abisheka, for their valuable advice, comments, and recommendations over the course of the project. I'd want to express my gratitude to all of the other lecturers in the department of IT for contributing critical expertise and assisting with the completion of this review paper In addition

Finally, I would like to thank all the unnamed parties who helped me in various ways for the successful completion of this assignment.

VIII. REFERENCES

1.Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. Traverse City: Ponemon Institute LLC; 2016. p. 1–50

2. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we? BMJ. 2017.

3. Alvarez M. Security trends in the healthcare industry. Somers: IBM; 2017. p. 2–18.

4. Millard WB. Where bits and bytes meet flesh and blood. Ann Emerg Med. 2017.

5. Argaw ST, Bempong N, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med Inform Decis Mak. 2019;5:1–11.

6. Ganten D, Silva JG, Regateiro F, et al. Science Has to Take Responsibility . 10 Years World Health Summit — The Road to Better Health for All; 2018. p. 6.

7. Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. Reuters. 2014.

8. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: a systematic review. Technol Health Care. 2016;24:1–9.

9. Health Insurance Portability and Accountability Act of 1996. Office of the Assistant Secretary for Planning and Evaluation

10. The Impact of HIPAA and HITECH. Mountain View: Symantec corperation; 2010. p. 1–7.

11. Regulation 2016/679 of the European parliament and the Council of the European Union. Brussels: Off J Eur Communities; 2016: 1–88.

12. EPFL IRGC. Governance of trust in precision medicine. Lausanne: EPFL International Risk Governance Center; 2018. p. 1–24.

13. Bradley N, Alvarez M, McMillen D, Craig S. Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations. Somers: IBM X-Force® Res 2016 Cyber Secur Intell Index. 2016: 1–19. 2017.

14. Cost of Data Breach Study, Global Overview. Traverse City: Ponemon Institute LLC; 2017. p. 1–34.

15. Steffen S. Hackers hold German hospital data hostage. DW. 2016

16. Zorz Z. Crypto ransomware hits German hospitals. Help Net Security 2016.

17. Khandelwal S. Nearly half of the Norway population exposed in HealthCare data breach. The Hacker News 2018

18. Hughes O. Norway healthcare cyber-attack could be biggest of its kind. Digital Health. 2018.

19. Irwin L. Breach at Norway's largest healthcare authority was a disaster waiting to happen. IT Governance Blog 2018

20. Warwick A. Norwegian healthcare breach alert failed GDPR requirements. Computer Weekly 2018.

21. Secureworks Counter Threat Unit Threat Intelligence. SamSam Ransomware campaigns. Secureworks. 2018. https://www.secureworks.com/research/ samsam-ransomware-campaigns. Accessed 29 May 2018.

22. Long S. The cyber-attack - from the POV of the CEO - Hancock regional hospital. Hancock Health 2018.

IX. AUTHOR PROFILE

WICKRAMASINGHE W A N

3RD Year 1st Semester Undergraduate in Bsc Honors Information Technology Cyber Security. Sri Lanka Institute of Information Technology.