The need for firm cybersecurity in healthcare

By Lakshman Thillainathan

Abstract – The lack of time, money and effort put into security within the healthcare industry is undeniably low. This article outlines previous and current research into cybersecurity threats in the healthcare industry comparing several articles.

Key words- Healthcare, Cybersecurity

i. Introduction

Healthcare organisations deal with highly sensitive information, they face challenges complying with tightening regulations, constantly facing cyber risks and adapting to digital transformation. As technology advances every passing day, risks to health organisations increase. Vulnerabilities in healthcare systems become much easier to detect and corrupt for anyone with malicious intent. Data can be stolen, data might get deleted or corrupted, in many cases these have not been obvious for years. Medical devices can get hacked, creating a high risk to patients. Patient medical records sell for thousands of pounds on the dark web, due to the fact they contain all sorts of important private data. Things like, date of birth, credit card information, addresses, emails, phone numbers etc, when information as important as this gets leaked, the victim can be affected for years.

For example, in 2017 the “WannaCry” ransomware encrypted files on over 230,000 computers in 150 countries. Even though the attack was not directed towards the NHS, it was the most effected. The attack led to disruption in one third of hospital trusts in England. There were several delays in test processing and communication of diagnostic tools and several other equipment affected. However, in response to the disruption, the NHS made several changes to the way in which they handle cybersecurity issues. They planned to remove and isolate unsupported software in the NHS. Even small changes such as informing NHS CEOs and CIOs when email services go down, (Smart, 2018) .

There are many reasons as to why healthcare is the biggest target for cyberattacks. I will be looking over a couple reasons and provide my analysis of the problem. Healthcare staff aren’t educated well with online risks, Healthcare information needs to be open and shareable as the information needs to be passed around the network to the required staff, outdated technology means the healthcare industry is unprepared for attacks. Its not only cyber-attacks that is putting the industry down, physical problems could also exist. Having monitored workstation uses, unique id’s and access controls are all apart of the physical safeguards that can be applied. In order for us to keep healthcare systems in check and protected, healthcare providers must be more aware and responsive to cybersecurity trends. Cyber attacks are up 125% since 2010 to 2016. Furthermore, with the coronavirus pandemic causing a ruckus to several industries, it made a huge impact on cyberattacks itself. The FBI have recently reported that the number of cyberattacks they hear about has had a 400% increase since pre-coronavirus.

ii. Related work

Clemens Scott Kruse (Kruse, Frederick, Jacobson, & Monticone, 2017) had the goal to identify cybersecurity trends and identify possible solutions by questioning academic literature. They first tried to find as many studies that has been done on “ransomware” or “cybersecurity” and found a total of 54 articles, then stripped it to find only useful ones. With all the information they gained, they concluded that the two main exposures for healthcare were, rapid technological advancement and evolving federal policy. The report was very useful in understanding the reasons as to why and how America's healthcare system has gone down the drain, but it lacks information from other countries, as other countries may have solved issues that they are struggling with, or have experience with dealing with vulnerabilities in healthcare. A more recent similar study by (Mohammad, Sabina, William, Perakslsis, & Madnick, 2019) concludes that a majority of articles on cybersecurity focus on technology and that human-based and organisational aspects were understudied. An overwhelming majority of cyberattacks are caused or initiated by humans. The article made me understand the lack of research in regard to physical security, these are very important as they could effectively affect the lives of patients.

Jay (Ronquillo, Winterholler, Cwikla, Szymanski, & Levy, 2018) have conducted research on the reports of ransomware and gains their information from federal law. In comparison to the previous articles that gained their information off of PubMed etc. The citing provided further statistical evidence to suggest the large increase in breaches of health information in America. There was a total of 364 breaches classified as hacking incidents that involved 130 702 378 patient records, that is an unbelievable amount of records hacked. It also showed that most of the breaches (91.5%) happened via the network server, pinpointing the main vulnerability.

Going back to the WannaCry ransomware attack, (Clarke & Youngstein, 2017) were doctors working at the time of the attack, having an inside perception of how and why it happened makes you understand how outdated and vulnerable the software in hospitals are. This citing went neck and neck with (Smart, 2018) as it provided context on the same incident. One was how it happened and an account of how stressful the situation was, and the other providing solutions and action plans to learn from the WannaCry attack. (Clarke & Youngstein, 2017) Stresses the underfunding that led to the disaster, Former Prime Minister, David Cameron, had elected to cut costs by scrapping a £5.5 million annual deal with Microsoft just so they can keep windows XP. It was clear that everybody, including the PM, did not anticipate the need for cybersecurity and just looked it away. With the coronavirus pandemic already putting healthcare workers at stress, it also caused stress to the cybersecurity of healthcare. (Muthuppalaniappan & Stevenson, 2020) have conducted research into the current situation of cybersecurity due to COVID-19, stating that with the COVID-19 vaccine development, modelling and experimental therapeutics become desirable to hackers. In response to the immense number of attacks and the importance of the data stored, the UK's Health Secretary gave the UK's intelligence service access to the NHS IT network. Providing information on unique cyber attacks and data breaches that happened in healthcare during the outbreak.

iii. Analysis and Critical Discussion

The NHS trust healthcare organisation consists of multiple user groups, all interconnected in someway. From the actual nurses and doctors in the front line of work, to the patients receiving their care, and even management executives are all vulnerable to the dangers of a cyber-attack. With 2,500 staff working, cyber-security is an important aspect. As we know from the WannaCry ransomware attack, when a worker opened the ransomware to set the whole thing off, that staff are not well educated on social engineering and the impact. It is a psychological thing to trust others when they "know" more, it is the same case when people use computers. Without patching the staff up with awareness of security, they become more prone to many sorts of attacks. As Kevin Mitnick said, "People are the weakest link". There are several ways in which human error could occur, someone can easily impersonate as a colleague or manager, they can send malware through emails, can be phished and there is many more. This could lead to the employee's data or organisation's data being breached and misused. Malware attacks have advanced significantly since the dawn of cyber-security, with some malwares being easily transferable. Let's say hypothetically that there was extremely strong security within the hospital, if a staff member had malware on their phones and went work with it, they risk the entire hospital from receiving said malware. Malware's will just pop up on their screens during operations asking for bitcoins, or whatever the malware specification, and disrupt doctors and nurses from operating. What if a patient was in a life or death situation and the crucial data needed is blocked of by the ransomware? It is highly important that the staff are aware of their potential actions. One security requirement should be for NHS employees is to use strong password protection and authentication. Putting in place password guidelines such as, having a minimum of 10 characters and must include numbers, symbols and capital or lowercase letters. As we do in the university of Greenwich, you should be required to change passwords every month, this will create smaller windows for hackers to breach staff accounts. Authentication should also be modified to make sure that only specified people are able to access certain data, maybe introducing keys for sets of data's so that only a few people have access to the information, and limiting the number of users able to access the information at once. With 300 beds in the hospital and several USB ports and other devices connected to each bed, it leaves a huge flaw for security. A patient could simply insert malware (through USB port) when left alone in the bed without any staff noticing. Having locks to make sure cables do not come off and blocking unused ports of access. Organisations should ensure all staff are aware of common cyber-attacks including: luring staff to download malicious software, phishing emails disguised as malware, spyware that is imbedded in any software. They should also be aware of using strong passwords, avoiding unknown emails and links, enabling and making sure firewall is up to date at work and home, and effective staff training. To protect them from having their phones stolen by potential attackers, they should have access to lockers to keep their mobile devices hidden.

Cyber-criminals can shut down servers, whole networks and devices and then demand ransom for the encryption. This may cause disruption to medical devices, appointment booking systems, patient records and other means of service. Any cyber-security breach can lead to the disruption of necessary data, this could include lifesaving emergencies. Patients in comparison to staff are more unaware of the potential risks they face. Furthermore, with data becoming more interconnected, and providing a more ease of access for patients, it increases the risk of phishing. For example, there can be phishing websites that masquerade the official NHS government site (also known as pharming). This is bad in several aspects, the website could be asking for personal details from the patient, and the patient can give permission to their information thinking that the website is trusted. There is also a possibility for attackers to create a phishing app related to the NHS and used to gain information from patients. Due to the ransomware attack in Australia, it is reported that every citizen medical record can be purchased on the dark web. We should learn from this and keep medical records safe for the patient. Research suggests that an individual's medical information is 20 to 50 times more valuable to cybercriminals than personal financial information. The patient's records include all sorts of information from their home address to their bank details, and obviously having millions of patients data leaked will upset patients. Patients could even simply refuse service from healthcare industries due to their paranoia of having their data leaked. Patients put their trust in an organisation to keep their data safe, breaking that trust in any industry could potentially put off customers from using their services. We can put some security requirements to make the patient more aware of issues, by providing text updates as to whether a phishing link has been going around and reminders that the NHS only send texts from a certain number and do not email. Informing the patients that there is no use for emails would make sure that patients know not to click any emails from NHS.

The Owner or any management executive of the NHS trust will also be vulnerable to data breaches. Healthcare software's typically include records of staff as well, including more data than a patients. The management can be targeted by a Denial-of-service (DoS) attack, where an attacker sends an abundance of connection or information requests. This would then overload the management and will stop them from being able to respond to legitimate requests for service, may even lead to system crashes or performance issues. This would leave them unable to communicate with other staff or acknowledge other issues going on in the hospital. If management services get disrupted, the staff will be confused with little guidance coming in from management. Furthermore, management is considered a trustworthy and direct route of information, so if a malicious actor thieves the identity of a manager, it becomes a big risk as the staff could be providing information to the thief rather than the manager. The management may also be targeted by Man in the Middle attacks, where an attacker monitors the network packets, modifies them and then put them back into the network, therefore information that may not be correct will be given across the hospital. A simple security requirement that can be implemented is a firewall. Firewalls are used as a major barrier that prevents the spread of cyber threats. It would be crucial that the managements computers are free of any malware, and to do this they could purchase antivirus software, and other means of security software. Having recovery drives set up in case of any change within software so that they can recover back to a version without the issue. With the advancement of software there is also tools that can be used to help filter emails to make sure there are no spam or unnecessary emails. Having unique email address domains for staff to use, insuring that only members of staff are able to use the domain address. e.g. "MarcusE34@NHS-management.co.uk".

Almost one fifth of healthcare providers, in the USA, do not have a leader solely responsible for information security and 25% of facilities do not have a security operation centre to identify and evaluate threats. In contrast, in the UK most hospitals have security operations that provide network safety. Security operations deals with all the security arrangements that are in place. Security operations should hold their own unique key card, this will provide them access to all the databases and networking rights. Having them monitor for any disturbance or change in a network, even having software that informs them when anything out of the ordinary happens within the network, also known as packet sniffers. Make sure that individuals can only access data and services for which they are authorised, further limiting who can access what. They should make sure that the security team is highly trained and responsive, with organisations monitoring who accesses what information.

iv. Conclusion

I have carried out research on cyber threats and attacks that have, and can happen to healthcare services, providing my input on what may be better or worse to try. To conclude, it is clear the cybersecurity in healthcare has been avoided for many years, this was due to the common decency that who would attack a hospital? However, with the age of technology, came the new "criminal" age, where criminals steal information, control machines in order to make money from exploits. Furthermore, with the coronavirus pandemic, many people have lost their jobs and therefore provides them with motivation to become a criminal. I believe the first step to solving the cybersecurity issues in healthcare, is to first acknowledge that we are in a time of technological advancement. It is not only healthcare systems that will become stronger and firmer, so will the hackers. Organizations hoping to comply with federal initiatives are spending around 95 percent of their IT budgets on implementation and adoption, while less than 5 percent of their IT budgets are spent on security, therefore begging for an increase in funding. Building a stronger incident report plan and business continuity plan should be the first main steps to mitigate threats. Cybersecurity has been accepted for many years in the risk control factor, and should change. Cybersecurity is essential in maintaining the safety, privacy and trust of patients. More money and effort need to be invested into ensuring better security practices. When designing new software for the hospital, consider security during creation rather than after it has been created. Insuring that there are regular backups and keeping software up to date, I mean for starters stop using windows xp. Investing in systems which support secure data transfer. Furthermore, as CISO you do not want data leaks to happen and then have countless law suits affecting the hospital.

References

[1] Smart, W., 2018. Lessons learned review of the WannaCry ransomware cyber attack. *Department of Health and Social Care, England UK, London*, *1*(20175), pp.10-1038.

[2] Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K., 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), pp.1-10. (Kruse, Frederick, Jacobson, & Monticone, 2017)

[3] Jalali, M.S., Razak, S., Gordon, W., Perakslis, E. and Madnick, S., 2019. Health care and cybersecurity: bibliometric analysis of the literature. *Journal of medical Internet research*, *21*(2), p.e12644.

[4] Ronquillo, J.G., Erik Winterholler, J., Cwikla, K., Szymanski, R. and Levy, C., 2018. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA open*, *1*(1), pp.15-19.

[5] Clarke, R. and Youngstein, T., 2017. Cyberattack on Britain's National Health Service—a wake-up call for modern medicine. *N Engl J Med*, *377*(5), pp.409-11. (Clarke & Youngstein, 2017)

[6] Muthuppalaniappan, M. and Stevenson, K., 2020. Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health. *International Journal for Quality in Health Care*.