Cybersecurity and Patient Safety: 
A Literature Review

Mohammad S. Jalali  
Keri Pearlson

Cybersecurity at MIT Sloan  
May 9, 2018

1. Introduction

Technology continues to advance in this digital age and with it comes the advancement and increase of cybersecurity attacks as well. According to Magrabi, F., M.S. Ong and E. Coiera (2016), “27% of respondents had at least one security breach over the past year, compared to 19% in 2010 and 13% in 2008”\(^1\). Even though the trends show that cybersecurity attacks are increasing, most hospitals still are not implementing adequate cybersecurity procedures to protect themselves from attacks. With the sensitive nature of medical data, one would think protection of such information would be a priority. However, that is currently not the case. For example, in a research paper by Verizon called “2018 Data Breach Investigation Report”, 79% of medical data is compromised, making it the most compromised followed by personal data (37%) and payments (4%). Reasons for such incidents are caused often in the form of mis-delivery of information (62%), followed by “misplacing assets, misconfigurations, publishing errors and disposal errors”.

However, misuse “in the form of privilege” happen in 74% of cases with 47% of people citing “fun or curiosity” and 40% citing financial gain as their motive. Because most hospitals have limited staff and are under-equipped, cybersecurity no longer becomes a priority. A paper written by Bai, Gopal, Nunez, and Zhandov (2012) found that "Despite large and diverse research on healthcare processes and information security, there is dearth of research addressing healthcare processes with the objective of achieving both the operational efficiency and meeting information security requirements.” With the lack of cybersecurity measures across hospitals and their high volume of patient information, hospitals become a desirable target for cybercriminals and are prone to cyber attacks and threats. While some hospitals do undertake some action in protecting their cybersecurity, their efforts are insufficient and, at times, outdated. Some hospitals might pursue research in cybersecurity, however, most of the research regarding this field focus on data breaches. There is no denying the importance of such studies, but there are elements in patient safety that have not yet been analyzed but should be investigated for the sake of protecting hospitals and individuals’ information.

2. Patient safety

2.1 Explanation of patient safety

In the context of healthcare, cybersecurity refers to the bodies of technologies used by hospitals, pharmacies, and other medical institutions to protect their records, networks, and medical devices. In this paper, we generally define patient safety, from the perspective of cybersecurity, as the level of security of a patient’s information, data, medical history, and

---


similar records. In other words, patient safety is ultimately about how well-protected patients are in their interactions with medical institutions.

2.2 Why we are focusing on patient safety

Patient safety must be further analyzed especially in relation to cybersecurity because this is a significant concern of which little to no attention is being provided. Currently, cybercrime is evolving to not only steal information, but also tamper with medical devices, electronic records, and other crimes. As a result, not only can a lack of cybersecurity measures result in stolen data, it can also cause financial loss, blackmailing, illegal increases in medication dosage, locked or uninterrupted medical devices, interrupted work operations, closed emergency rooms and other hospital departments, canceled surgeries, and other events (some of which could lead to the result in further and more lethal consequences). Incidents such as the one aforementioned damages the hospital’s reputation and, in most cases, affects their finances due to the millions that were either stolen from them or were paid to settle lawsuits and cases. Additionally, hospitals’ lack of focus on cybersecurity and patient safety leaves them extremely unprepared in the event of a massive cybersecurity attack. For example, to prevent such situations, there needs to be a contingency plan and, currently, no research has been conducted on such situations. Due to the gravity of the situation and its consequences, it is crucial to investigate how institutions can be better prepared to safeguard their most valuable asset: their patients.

3. Research question

The main question of this research then becomes, with all the red tape and restricted funds, how can medical institutions best handle cybersecurity with the safety of patient
information as the priority? In addition, what vulnerabilities, if any, do technologies used in hospitals have?

In order to answer the questions that we have, we use a survey analysis. In this survey, there are several categories with each question designed to understand what is currently done, what needs to upgrade, and what can be done about it.

4. Research methods

In order to find appropriate information that was relevant to the research, two separate databases were chosen by the researchers: PubMed and Google Scholar. The search string used in PubMed included a mixture of the words “patient”, “safety”, “harm”, “cybersecurity”, and “cyber-attack”. A similar search string was used with Google Scholar.

Topics that were considered to be relevant to the research included the role of governance and leadership, awareness and training, identity and access management, asset management, medical device security, electronic health record systems, risk management, network security, contingency planning, and physical and environmental control in overall cybersecurity measures, or lack thereof, in hospitals to protect their patients. After accounting for duplicates, a total of 150 references were amassed through EndNote. From that population of data, we gathered a sample of 12 total sources that were relevant to cybersecurity and patient safety. The data collection procedure lasted approximately one to two weeks.

5. Review of Literature/Result

This section provides a detailed review of all of the articles that were analyzed in this research. All of the following articles are in agreement that cybersecurity is a growing concern, especially in medical institutions. This section is organized by first looking at papers which give
a general overview of why cybersecurity must be prioritized and then delves into research that
analyzes what improvements could be made to cybersecurity in healthcare. Lastly, this review
ends by looking at research articles which investigate more specific cyber attacks both in certain
medical industries and in other countries.

5.1 The importance of prioritizing cybersecurity

Information is precious, and along with the advancement of technology comes the
increasing value of data. The medical data that is obtained from patients is no exception to this
notion. To put into perspective how valuable medical information is, according to Clemens, S. K.,
Frederick, B., Jacobson, T., and Monticone, K. D. (2015), thieves find patient information to be
20 to 50 times more valuable than person financial information\(^4\), yet most hospitals do not do
enough to protect such data. In fact, the aforementioned researchers note that even if hospitals
were investing some effort, money, and resources into cybersecurity, most organizations end up
allocating most of their budget to implementation (95%) rather than security or protection (5%).
As a result of insufficient security measures, cybersecurity attacks are becoming not only more
common, but also more dangerous.

A more specific example of why hospitals should prioritize their cybersecurity is because
of the dangers of medical device tampering, which is the second most common cyber attack\(^5\).
Currently, medical devices are created without features that protect them from third-party
influences, thereby leaving them defenseless and easy to hack. In a research conducted by
Middaugh, D. J. (2016), “only 26% of the respondents reported that they used security of


medical devices as part of their cybersecurity plans” and that the quality of security around medical devices is estimated to be about a decade behind the overall standard. Additionally, individuals at the Mayo Clinic conducted research on medical devices and found that majority of the equipment such as ventilators, MRI scanners, ultrasound equipment, electroconvulsive therapy machines, and many more have defenseless operating systems. Middaugh (2016), also notes that, in 2013, security researchers demonstrated how several medical devices such as wireless insulin pumps could be tricked “into delivering a lethal dose of insulin”, and wireless pacemakers could be manipulated into delivering “a deadly shock”. With an expected 7.7% increase in individuals who need implantable medical devices by 2015 and with over 2.5 million individuals who already currently rely on them, it is extremely crucial that hospitals invest more time into building more secure operating systems for their tools. Otherwise, they leave themselves vulnerable to a multitude of possibilities which could result in the loss of human lives.

5.3 Examples of cyber attacks in medical industries and other countries

Cybersecurity attacks are not just familiar to brick and mortar hospitals. Online medical organizations are also no stranger to them. For example, a growing trend in the field of medicine is e-commerce and online pharmacies, which ships prescriptions to patients who can buy them online. However, Mackey, T.K. and Nayyar, G. (2016) note the lack of cybersecurity pursued by these websites in order to protect customer information. For example, they mention that 80% of 60 online websites reviewed “had either critical or medium-level vulnerabilities that do not provide

---

adequate protection for online consumers”\(^9\) and that “17% of Internet pharmacies failed to provide a secure site”\(^10\). Moreover, according to Mackey and Nayyar, online pharmacies are part of a much larger organized crime network that use cyber attacks to “engage in financial fraud and data phishing activities”\(^11\).

Cyber attacks are also prevalent in countries other than the United States as well. In a paper by Martin, G., Kinross, J., and Hankin, C. (2017), they note the lack of cybersecurity in the United Kingdom along with the failure of the National Health Service (NHS) and the United Kingdom’s government to solve these problems. Like the hospitals in the United States, many organizations under the NHS only dedicate 1-2% of their annual budget on IT, while 4-10% is spent on “other critical sectors”\(^12\). Of that small portion, an even smaller portion is allotted to security measures. Due to the lenient culture of NHS organizations toward cybersecurity, many cybercriminals have attacked their infrastructures, causing inestimable damage. One example is the recent global attack called WannaCry, which globally affected over 200,000 computers in 150 countries\(^13\). However, hospitals in the United Kingdom were also severely affected due to the fact that the WannaCry ransomware attacked computers that utilized the Microsoft Windows operating system. At the time, many NHS organizations were still using Windows XP, “which has not been secure since the government chose not to extend the £5.5m (€6.4m; $7m) support deal with Microsoft in 2015”\(^14\). Because the UK government and the NHS are doing little to improve their cybersecurity measures, Mackey and Nayyar state that their actions have “resulted in a prolonged time at risk”,

much like a ticking bomb. They conclude that the best way to truly protect medical institutions and patients from attacks such as WannaCry is to create effective cybersecurity measures and to call for more effective leadership on cybersecurity.

5.2 Potential improvements to cybersecurity in healthcare

When it comes down to how to protect patient information, there are actions that an institution can take. A study done by Gerard, P., Kapadia, N., Acharya, J., Chang, P. T., and Lefkovitz, Z. (2013) looks at how information through wireless networks are transferred and the preventative measure that could be taken to maximize security. They also discuss the settings and features that the average computer or mobile device should be adjusted to. Another study by Ross, J. (2017) gives advice on how to improve cybersecurity systems by giving tips on multiple aspects of cybersecurity. Ross advises readers to work in conjunction to their IT department to better train their staff, create a contingency plan, routinely update several security-related aspects in their networks such as their antivirus software and passwords, and more. The article also briefly talks about past cybersecurity attacks and predicts trends in cyber attacks.

As for management structure, Bai, X., Gopal, R., Nunez, M., and Zhdanov, D. (2014) look at how to minimize risk in a situation where the number of healthcare professionals is not growing fast enough to cover patients and their security needs. An example of a patient visit at a physician’s office was given and there were a list and analysis of all the things to look out for: security conflict, disclosure risk, and control. The findings in this study were to first and foremost maximize efficiency by allocating tasks to the appropriate skill levels and then to have a workflow model to minimize liabilities and cost.

There are plenty general efforts that one can make as listed above but there are also specific improvements that can be made. He, M., Devine, L., and Zhuang, J. (2018) discuss the
benefits and costs of information sharing between governments, public, and private sectors, and illustrates such benefits and costs through 15 scenarios. This research concluded that using the NIPC (National Infrastructure Protection Center) and ISAC (Information Sharing and Analysis Center) to exchange information would help companies to improve their cybersecurity. Another study by Collmann, J., Coleman, J., Sostrom,K. And Wright, W. (2004) evaluates ways to best ensure that technologies in organizations are safely managed. There are two systems, OCTAVE, a self-directed information security risk assessment process, and RIMR, a Web-enabled enterprise portal about defense health information assurance, that would assure a more defensive health information system. Going off the ideologies of the military health system, it was found that repeated safety measures, training and education of employees, and strong leadership would most enhance the safety of organizations.

6. Discussion

4.1 Summary of evidence

Overall, the evidence we have gathered support the notion that cybersecurity attacks are increasingly becoming a concern not only in the United States, but in other countries as well. One consistent pattern that is shared among the research papers is that medical institutions are not using sufficient methods to protect patients and their information. As a result of the relaxed mindset hospitals possess towards cybersecurity, hospitals are extremely vulnerable to cybercrime. Additionally, this literature also stresses the importance of finding ways to improve multiple features of hospitals such as, but not exclusive to, electronic health records, security of medical devices, information management, organizational leadership and training, identity and access management, network security, contingency planning, cybersecurity training, and risk management. While this literature equally stresses on the importance of improving all
aforementioned facets of medical institutions, the greatest emphasis is placed on hospitals improving and being more proactive with cybersecurity measures.

4.2 Limitations

Some limitations that the researchers experienced was that research papers that focused broadly on cybersecurity and patient safety were hard to find. Instead of finding general papers, what researchers found instead were many articles that focused on a specific aspect of cybersecurity in relation to health care. On the other hand, when the researchers did find a paper that was an overview of cybersecurity and patient safety, they discovered that the paper was not very detailed due to the nature of cybersecurity being a very broad subject in general. As a result, this literature was not able to include all of the cyber threats and suggestions for cybersecurity improvement.

4.3 Conclusions

As technology advances, so do the tools used by cybercriminals to hack into the medical data of hospitals and patients. The fact that many hospitals are understaffed and under protected causes them to be the most vulnerable to such threats. Additionally, the longer that hospitals wait to improve their security systems, the more prone they are to future cyber attacks. Therefore, hospitals must prioritize patient information security and allocate more resources to their cybersecurity infrastructures. More specifically, medical institutions must improve their governance and leadership, awareness and training, identity and access management, asset management, medical device security, electronic health record systems, risk management, network security, contingency planning, and physical and environmental control.