**Semester Research Project: Cybersecurity in Hospitals**

Natalie Waugh  
University of South Florida  
LIS 4934 BSIS Senior Capstone  
Dr. Vanessa Reyes  
July 20, 2023

**Introduction**

The hospital system is an incredibly complex organization that requires an effective and efficient cybersecurity framework in place to run operations smoothly. The sensitivity of a hospital’s information makes it imperative to improve cybersecurity practices and to maintain compliance with privacy and HIPPA laws. The question is, what is required to manage an efficient cybersecurity infrastructure in the hospital system and what challenges exist?

A cybersecurity system is vital to protecting patient information in a hospital system, and requires effective security policies, ongoing education, and diligence to defend against evolving cyber-attacks. Goals for this research project will include identifying cybersecurity challenges and vulnerabilities, current cybersecurity practices, pertinent policies, need for ongoing cybersecurity education, and any recommendations. The focus is to explore the landscape of cybersecurity within hospitals and discuss recommendations for improvement. Throughout the paper, research and literature will be examined and analyzed to gain insight into this topic.

**Use of Electronic Health Systems**

Hospitals and nearly the whole healthcare system have become increasingly reliant on technology and digital devices to deliver healthcare services. The benefits of this phenomenon have been quicker and more reliable delivery of patient care services and the ability for healthcare professionals to access information electronically. The drawbacks are escalating threats from malicious hackers and the growing complexity of security challenges. This requires effective cybersecurity practices to maintain defenses and a strong network.

There has been a shift to electronic system usage in hospitals over the last couple decades. The use of Electronic Health Records (EHRs) has changed the way hospitals operate and deliver services in a profound way. EHRs allow healthcare professionals in the hospital to record, document, and store valuable patient information electronically. This has largely replaced paper methods of patient care documentation. The use of EHR systems has led to an improved quality of hospital care due to quicker delivery of healthcare services. However, studies have shown a lack of digital literacy and absence of a strong cybersecurity system is detrimental to patient care when using these electronic systems (“Improving EHR System Affects Patient Care”, 2011).

That is why it is vital to devote funding and resources to improving EHR capabilities, strengthening cybersecurity, and establishing a dedicated Information Technology/Information Security Team in hospitals. It is also important to train healthcare staff on using these electronic health record systems to maximize benefits while minimizing unintended consequences due to lack of digital literacy. Improving EHR systems is essential to preventing data breaches and protecting patient information.

**Cybersecurity Challenges and Vulnerabilities**

Concerns regarding escalating cyberattacks in hospitals prompt the need for advanced cybersecurity measures. It is no secret that without proper protections and defenses in place, patient information is at risk and the ability to deliver healthcare services safely is threatened. The reliance on electronic systems in hospitals means that any data breach or malicious attack has a negative impact on the ability for healthcare staff to do their job effectively. The challenge for hospitals is keeping up with escalating attacks and devising innovative ways to improve cybersecurity measures.

Hackers are only becoming savvier over time and have garnered increased attention in mainstream media. Cyberattacks in healthcare and hospitals are especially dangerous because of the sensitivity of the targeted information. Personal health information (PHI), such as name, social security number, birthdate, and health information, cannot simply be reset or changed if hacked. Patient safety is the focus when implementing cybersecurity measures in hospitals. A risk assessment approach is helpful because it identifies vulnerabilities and potential security risks. Literature also mentions that a multi-disciplinary approach is essential to improving cybersecurity, which includes hospital executive leadership, hospital staff, information security/ information technology teams, and medical device manufacturers (Argaw et al., 2020).

Common cybersecurity threats that hospitals face include attacks such as email phishing attacks, ransomware attacks, loss or theft of equipment or data, and attacks against connected medical devices. A compelling research study developed an evaluation model to evaluate existing cybersecurity practices in hospitals. This evaluation model is helpful for determining where a hospital ranks in cybersecurity and allows potential areas for improvement to be revealed (Ahmed et al., 2022). The awareness of these threats allows hospitals to practice diligence when using electronic systems. The hope is that vulnerabilities will be identified with measures taken to improve cybersecurity measures before attacks happen. Having cybersecurity awareness would also prevent hospital staff from falling prey to social engineering attacks and practice good security habits.

The Covid-19 pandemic brought unforeseen security challenges and hardships to an increasingly vulnerable healthcare system. Hackers exploited these vulnerabilities during this stressful period. Some of the challenges that stood out were security vulnerabilities due to remote work, limited funding or resources, lack of security awareness, and an increased demand for medical supplies. The pandemic brought an increased need for Personal Protective Equipment (PPE) in hospitals and suffered from a massive shortage. As a result, hospitals faced an increase in digital scams related to PPE and medical supply fraud (He et al., 2021).

**Cybersecurity Practices**

Several cybersecurity practices became apparent in the literature when analyzing the responses made by security professionals in hospitals. One of the practices that stood out to me was the effort to bring awareness to security issues and concerns. This is thought to promote caution and attentiveness from staff and users. Education on cybersecurity practices would include having a strong password, keeping login information concealed, and logging out of devices when not in use. Other practices included setting up a strong information technology and/or security department to maintain the security infrastructure and fix issues that arise. From a purely technical perspective, practices such as intrusion detection systems, firewalls, antivirus, log event monitoring, network auditing, segmentation, privileged access restrictions, and multi-factor authentication measures are beneficial to preventing and responding to malicious threats (Argaw et al., 2019).

These cybersecurity practices demonstrate both practical and technical approaches to protecting sensitive information and preventing cyberattacks in hospitals. Challenges exist when providing standardized protections throughout hospital systems or being able to keep up with escalating attacks. This is especially the case when hospitals rely on various interconnected medical devices or the Internet of Things (IoT). This includes electronic medication dispensers (Pyxis machine), diagnostic machines, tablets, work cell phones, and even vital machines. It is also a challenge to implement security policies and protocols to address each unforeseen security threat.

**Cybersecurity Policies**

Policies and procedures are necessary to provide guidance and regulations regarding cybersecurity defense. Drawing up pertinent policies and procedures is an ongoing progress in a hospital because it requires feedback and evaluation of the cybersecurity system. This results in some challenges because policies need to address not only data privacy but also information security itself.

Policies set the standards of conduct and behavior regarding the use of hospital devices and following cybersecurity practices. This may include practices to be followed by employees, procedures to be followed by the IT/Information Security Department, and guidelines on how to report cybersecurity incidents. Security policies can also set clear roles and responsibilities for those in a cybersecurity team. Experts propose policies that call for equal resource availability and standardization across hospitals. This would hopefully result in decreased inequity of available cybersecurity practices and technologies between hospitals. Security policies would also be required to address any unprecedented issues such as attacks, as well as an incident response plan (Jalali & Kaiser, 2018).

Strong cybersecurity policies are necessary to uphold the protection and privacy of patient information in hospitals. Since cybersecurity is a relatively recent phenomenon and field, developing strong cybersecurity policies is still an ongoing process that responds to trial and error. It also is meant to be updated and improved in response to new threats or unforeseen situations. Cybersecurity without policies in place is ineffective at protecting a hospital’s sensitive information.

**Cybersecurity Training in Hospitals**

In recent years, more emphasis has been placed on training hospital staff due to the widespread use of technology and electronic health systems to perform job duties. Hospitals have shifted from paper documentation and charting methods to mainly electronic forms of documentation and EHRs. This requires educating hospital staff on digital literacy and the security challenges faced when using these devices. Employees could fall victim to social engineering attacks such as email phishing and attackers posing as authorized personnel. This requires education and training to teach employees how to detect these attacks. Training includes simulated phishing exercises, training videos, and examinations provided by hospitals, with them being repeated yearly or as needed. This presents an opportunity to identify a lack of security awareness and potential for further education. Other educational opportunities include pertinent security policies, procedures on how to report incidents to the chain of command, and best digital practices. Best digital practices would be maintaining a clean desk with login information hidden, logging out of devices when not used, strong password policies, and avoiding suspicious links (Argaw et al., 2020).

Ongoing training is crucial to identifying weaknesses or gaps in knowledge, providing an education plan, and improving existing cybersecurity tactics. Cybersecurity is only as strong as the people who use it. Another way of putting it is, it doesn’t matter how updated or current a hospital’s cybersecurity measures are. It will still fail if users are not educated on vulnerabilities and how to avoid cyberattacks. This leaves the entire organization susceptible to attacks and threatens the privacy of its information, thus leading to potential patient harm. In my experience as a hospital employee, yearly training programs and mock phishing exercises were helpful in improving cybersecurity awareness and looking out for common social engineering attacks. This allowed the hospital staff to learn from mistakes and identify areas that needed to be improved on.

**Recommendations**

Through analyzing the literature and cybersecurity methods practiced by security professionals, it revealed that there is a constant need for innovation to respond to evolving and escalating cyberattacks against hospitals . This requires a strong Information Security/Information Technology Department in place with a team of cybersecurity professionals.

Some recommendations start with ongoing education of cybersecurity professionals, through certifications, training, and on the job experience. Risk identification and management is also essential to analyzing any potential weaknesses or threats in the cybersecurity framework to prevent any malicious attacks. Early vulnerability detection and patching actions would hopefully reduce the need to mitigate incidents. Compliance with software updates and collaboration with hardware manufacturers also promotes keeping up with cybersecurity defenses and minimizing risks. Educating the hospital employees through security awareness and training programs would also decrease the risk of falling victim to social engineering attacks. Education on best digital hygiene practices would also be helpful for minimizing security risks. Promoting resource equality and funding across hospitals regarding effective cybersecurity tactics would also strengthen defenses. Sharing cybersecurity incidents, practices, and solutions between hospital security teams gives them the opportunity to improve methods and learn from each other (Argaw et al., 2019). This would create a unified front against malicious attacks and reduce the chance for weak points to be exposed. A hospital cybersecurity registry would possibly be an effective approach for sharing security ideas and solutions.

Cybersecurity implementations measures should comprise of risk identification and assessment, intrusion detection systems, log event monitoring, network audits, firewall implementation, antivirus scans, network segmentation, privilege access restrictions, dual-authentication methods, and software updates (Argaw et al., 2019). This is only a few of several cybersecurity methods and approaches to defend a system from attackers. It requires a complex and organized framework with constant evaluation of effectiveness. A combination of these methods would allow security professionals to practice diligence and detect any suspicious behavior. It would also ensure that cybersecurity defenses would be provided on all fronts.

Cybersecurity policies should set guidelines, roles and responsibilities, and behavioral expectations on how to maintain a secure environment. Protocols should define how to report incidents to the chain of command and cybersecurity department. It should also state consequences for intentionally not following policies and procedures. This applies to all members of a hospital organization, including employees, leadership, and executive roles.

The most important recommendation in my opinion is to always commit to lifelong learning when developing a strong cybersecurity system in hospitals. It requires constant innovation and education to combat the escalating threats and attacks targeting hospitals. This would also be possible to achieve when there is an open dialogue between security professionals, where they communicate any incidents that occurred and the successful cybersecurity measures in response.

**Conclusion**

A strong cybersecurity system is crucial for a hospital to protect patient information and perform healthcare services safely and efficiently. It is a complex landscape that requires a team of security professionals, ongoing education, constant evaluation, and innovation to defend against escalating attacks. Hospitals are in a unique position because of the sensitivity of their information, which requires an urgency to protect personal health information and the privacy of patients. The shift from paper documentation to electronic health records and technology incorporation also caused an urgent need for developing effective cybersecurity practices. Aspects of developing a strong cybersecurity system includes identifying cybersecurity challenges and vulnerabilities, strong cybersecurity practices, pertinent policies and procedures, and ongoing security awareness training in hospitals. Cybersecurity is an ongoing effort to maintain the safety of hospitals and requires a commitment to lifelong learning.

**References**

Ahmed, M. A., Sindi, H. F., & Nour, M. (2022). Cybersecurity in hospitals: An evaluation model. *Journal of Cybersecurity and Privacy*, *2*(4), 853–861. https://doi.org/10.3390/jcp2040043

Argaw, S. T., Bempong, N.-E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. *BMC Medical Informatics and Decision Making*, *19*(1). <https://doi.org/10.1186/s12911-018-0724-5>

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O&rsquo;Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020, July 3). *Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks - BMC Medical Informatics and Decision making*. SpringerLink. https://link.springer.com/article/10.1186/s12911-020-01161-7

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021, April 20). *Health Care Cybersecurity challenges and solutions under the climate of covid-19: Scoping review*. Journal of medical Internet research. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8059789/

Improving EHR System Affects Patient Care. (2011). *Information Management Journal*, *45*(2), 10.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, *20*(5), 1–16. <https://doi.org/10.2196/10059>