Robel Degefa

Professor Yalpi

CYSE 201S

Article Review #2

How Technological Advancements in Healthcare have Increased the Risk of Information Theft

Introduction

We have seen in many fields how technological advancements have benefited companies, departments, profits, and businesses. But what is not talked about, is how many risks have been brought to light with the advancements in technology. The biggest, and the one I will be discussing regarding the article I read, discusses the risks and effects of technological advancements in our healthcare systems. Medical records are some of the most important and private pieces of information a human can have and at one point, these records were filed on papers stored in hospitals. As technology advanced, it presented easier and more convenient ways to store and keep track of information. This advancement led to medical records being stored online. Although the records are fully sealed and private, all hackers need is for it to be online and it will have vulnerabilities. The article studies the vulnerabilities that surround healthcare regarding information security and discovers the motivation in the hacking itself.

Importance Of Cybersecurity in Health Care

We have thousands of health institutions in America and there are important things that differentiate a good and bad facility. An important factor into why a patient would go to a hospital and not the other could be simply down to information security and how secure are your medical records. Medical records contain things like your banking, address, social security and more and when those things get into the wrong hands, the aftermath can be drastic. In the article I reviewed, it states a situation where a cyber attack on the US billing and payment system caused a large outage and millions of patients' information to be leaked “Cyberattacks on the U.S. healthcare system represent some of the most significant and consequential threats to the industry. A recent cyberattack in February 2024 targeted the largest U.S. billing and payment system, disrupting the processing of millions of patients’ prescriptions and services, which delayed access to essential medications and care (George et al., 2024). This situation not only jeopardized patient safety but also threatened the financial stability of numerous medical practices through lost revenue from unpaid claims, which could potentially restrict patient access to medical services.” (Yashna et al., 2024).

Conclusion

In conclusion, This article touched on a subject that many are not aware of and should be as every American citizen most likely has their information stored somewhere in a database under cyber encryption. It is amazing to see what technology has done and what it has in store for the future, but it is important to note that it is not perfect and comes with flaws. Our healthcare

system will always be one of the biggest targets for cyber attack and this article noted that and showed important measures that we need to take to keep our information safe.

References

Yashna Praveen, Mijin Kim, Kyung-Shick Choi,(2024) *Cyber Victimization in the Healthcare Industry: Analyzing offender motivations and Target Characteristics through Routine Activities Theory (RAT) and Cyber-Routine Activities Theory (Cyber-RAT)*. [International Journal of Cybersecurity Intelligence & Cybercrime],[Volume 7 (Issue 2)] Cyber Victimization in the Healthcare Industry: Analyzing Offender Motivations and Target Characteristics through Routine Activities Theory (RAT) and Cyber-Routine Activities Theory (Cyber-RAT)