How Can We Keep Our Patients Safe? Managing Cyber-Threats Post-Pandemic

cjni.net/journal/

Trends and Issues in Nursing Informatics Column

By Melanie Neumeier RN MN

Melanie Neumeier is an Assistant Professor in the BScN Program at MacEwan University in Edmonton, Alberta. Her research interests include integrating new technologies into nursing education and interdisciplinary collaboration in enhancing evidence-informed nursing practice. Melanie first became interested in nursing informatics through a nursing informatics course she took in her MN program at Memorial University in Newfoundland, and has since continued that interest in her research, her writing, and her teaching.

COLUMN

Citation: Neumeier, M. (2023). How Can We Keep Our Patients Safe? Managing Cyber-Threats Post-Pandemic. Trends & Issues in Nursing Informatics Column. *Canadian Journal of Nursing Informatics, 18*(1). https://cjni.net/journal/?p=10854

The COVID-19 pandemic has created unprecedented challenges for the healthcare industry worldwide, including an increase in cyberattacks. Canadian hospitals have been particularly hard hit by ransomware attacks, which have surged during the pandemic. Ransomware attacks can have serious consequences, including the disruption of patient care and compromise of sensitive patient data. There have been several recent ransomware attacks on Canadian hospitals that highlight the seriousness of this threat. Attacks on the University of Ottawa Heart Institute and the Newfoundland and Labrador health system in 2021, Toronto Sick Kids Hospital in December 2022, and Ross Memorial Hospital in February 2023 are just some examples of recent cyberattacks on healthcare targets (CBC News, 2021; Mosleh, 2023; Solomon, 2022). And while LockBit apologized for the attack on Toronto Sick Kids Hospital in December (Mosleh, 2023), the increase in frequency and scope of ransomware attacks on our healthcare system is a national concern. The Communications Security Establishment, the federal government's IT security agency, has noted that ransomware and other malware attacks are not only becoming more frequent, but are also becoming more sophisticated, and hospitals have some unique factors that make them vulnerable and attractive for cyber criminals (CBC News, 2021).

During the pandemic hospitals were forced to rely more heavily on digital technology to provide care and communicate with patients. That combined with an increase in remote work created new vulnerabilities that cybercriminals could exploit. Remote work often involves using personal devices and unsecured networks, which can make it easier for cybercriminals to gain access to hospital networks, especially if staff have poor password hygiene. Staff that

are already stretched to the limit may not receive adequate cybersecurity training, making them more vulnerable to phishing attacks or other social engineering tactics used to gain unauthorized access. Combine that with critical staff shortages and lack of resources, and it becomes very difficult for hospitals to maintain their cybersecurity defenses and respond to cyberattacks.

In addition to the stresses brought on from the pandemic there are several other factors that make Canadian hospitals vulnerable to ransomware attacks. One key factor is that many hospitals still use outdated software and operating systems, which can contain vulnerabilities that can be exploited. These vulnerabilities allow cybercriminals to gain access to hospital networks and install ransomware. Hospitals may not have adequate backup and recovery systems in place, which makes it more difficult to recover from a ransomware attack, and the need to have systems back up and running quickly to limit disruptions to patient care increases the chance that hospitals will pay the ransom, making them an attractive target. Working with third-party vendors that have access to hospital networks can create additional vulnerabilities if these vendors do not have strong cybersecurity measures in place. And with large amounts of valuable data being stored in healthcare systems, even if hospitals don't pay the ransom, selling the stolen data can still be profitable.

To mitigate the risks of ransomware and protect patient care, hospitals must prioritize cybersecurity. They should implement robust measures, including regular backups, encryption, multi-factor authentication, and training for employees on how to recognize and avoid phishing attacks. Hospitals should also regularly update their software and operating systems to patch known vulnerabilities, and ensure any third-party vendors have robust cybersecurity measures in place. In addition, hospitals need an incident response plan in place to minimize the impact of a ransomware attack and prevent disruption to patient care in the event of a breach. Regular vulnerability assessments and penetration testing can also help to identify and address security weaknesses in the system.

This kind of digital threat is not going to go away and as healthcare technology continues to evolve, the importance of protecting patient information and maintaining the integrity of EMR systems will only grow. Hospitals need to take steps to reduce the risk of ransomware attacks to protect our operating systems so that we can provide the best care to our patients and protect their personal information.

References

CBC News. (Nov. 4, 2021). *N.L. health-care cyberattack is worst in Canadian history, says cybersecurity expert.* https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyber-attack-worst-canada-1.6236210

Mosleh. O. (Jan. 5, 2023). *SickKids attack — and apology — pulls ransomware's 'Robin Hood' into spotlight*. Toronto Star. https://www.thestar.com/news/canada/2023/01/05/sickkids-attack-and-apology-pulls-ransomwares-robin-hood-into-spotlight.html

Solomon, H. (Dec. 22, 2022). *Toronto children's hospital confirms it was hit by ransomware*. IT World Canada. https://www.itworldcanada.com/article/breaking-news-toronto-childrens-hospital-confirms-it-was-hit-by-ransomware/519357