Perspectives

Jasmiry Bennett

HEALTHCARE CYBER ATTACKS

Every wonder what goes on behind the scenes in the cyber world? Healthcare organizations are under constant surveillance in protecting all patient healthcare information. Any breach in patient information can significantly impact a healthcare organization's reputation. Ransomware is a type of malware preventing healthcare organizations from accessing parts of their electronic healthcare record (EHR) by encrypting files in return for money.[1] When this happens, this can negatively impede patient care whereby causing delay in care and potentially harming patients. After encryption into an EHR, cybercriminals demand monetary compensation in return for release of protected information. If not paid, there is a threat to publically release protected information, leaving no choice but to pay. Even after payment, it is not guaranteed, cybercrimainals will release the encryption key. According to Spence et al (2018), it was estimated in 2016 more than $1 billion has been paid in ransomware.

There are four risk categories for concern with ransomware: medical malpratice, data privacy, property and reputation, and cost and expense. Medical malpractice increases when EHR systems are inaccessible, thus increasing the risk of medication errors potentially causing an adverse effect to patients.[1] Data privacy is a huge concern as healthcare systems can potentially violate Health Insurance Portability and Accountability (HIPPA).[1] Property and reputation becomes a challenge for future business negotiations and partnerships, as trust in an organization is perceived as turbid. Lastly, cost and expense can pose a financial hardship for healthcare institutions paying cybercriminals. In addition, healthcare institutions are held responsible for continued monitoring of patient information and credit monitoring.[1]

As healthcare providers, we are all ambassadors in protecting our patients and our healthcare organization. Cybercrimimals are well aware of the high vulnerability in healthcare and low threshold for payment; thus healthcare organizations are an easy target. I encourage all to report any breach concerns and continue awareness, as proper risk mitigation and disaster recovery plan is everyone's responsibility.

Jasmiry Bennett, DNP, RN, ACNP-BC
Editor-in-Chief

REFERENCE

1. Spence N, Bhardwaj N, Paul DP III, et al. Ransomware in healthcare facilities: A harbinger of the future. Perspectives in Health Information Management; 2018. http://perspectives.ahima.org/wp-content/uploads/2018/06/RansomwareinHealthcare.pdf.

J Vasc Nurs 2019;37:225.

1062-0303/$36.00

https://doi.org/10.1016/j.jvn.2019.12.001