The 12th Annual Dupont Summit on
Science, Technology, and Environmental Policy

Friday, December 6, 2019
The Historic Quaker Meetinghouse
2111 Florida Ave. NW, Washington DC

Title: This Type of Epidemic in Healthcare Requires an Information Security Plan

By

Calvin Nobles, PhD
Cybersecurity Fellow
New America Think Tank
Calvin@CalvinNobles.com

James J. Williams, PhD
Researcher/Cybersecurity Professional
jjwilliamsphd@gmail.com

Overview:

The growing epidemic of cyber and ransomware attacks in healthcare does not require a treatment plan; instead, it mandates an Information Security Plan. The healthcare industry is capitalizing on digital transformation resulting in unprecedented amounts of data. Existing research indicated that "the two primary drivers exposing healthcare to cyber threats include rapid technological advancement and evolving federal policy. As healthcare IT infrastructure struggles with new technology and security protocols, the industry is a prime target for medical information theft" (Kruse, Frederick, Jacobson, & Monticone, 2017, p. 8). The interconnectivity of medical devices, healthcare systems, and increasing digitalization (Williams & Woodward, 2015), challenge the healthcare industry from a security perspective given the mounting targeting of medical information by cybercriminals.

Another critical concern for healthcare is securing digital devices, which Davis (2019) argues that accounting for the security of digital assets is an organizational-level issue and requires strategic development efforts and business initiatives to mitigate the threats and vulnerabilities. Technological innovations such as (a) digital solutions, (b) health monitoring systems, (c) mobile applications, (d) electronic medical records, and (e) mobile personal health records (Karampela, Ouhbi, & Isomursu, 2018) provide real-time and extensive access to patient data; consequently, creating data and network security issues for healthcare organizations (Haggerty, 2017).

Haggerty (2017) asserted that the healthcare industry is experiencing significant growth in digital services, which increases the reliance on software applications that continues to plague the existing complexity of network infrastructure, data management, and privacy issues for healthcare organizations. Information security, technology, and risk executives in the healthcare domain should develop strategic initiatives to address the influx of health data generation capabilities.

The cost of medical and health information on the dark web continues to increase in value. The price of a health record on the dark web can sale as much as $1000 (Stack, 2019), which is more than credit card data (Davis, 2019). Some researchers and practitioners emphasize that medical information is 20 to 50 times more valuable than credit card data (Kruse et al., 2017). The proliferation of some cyber-attacks in healthcare stems from onboarding once stand-alone medical systems that lack adequate security protection to a hyperconnected environment (Kruse et al., 2017). Even as medical device manufacturers are diligently addressing the security mechanisms in digital and medical devices (Kruse et al., 2017), the failure to keep pace with the malicious threats allows the cybercriminals to have the strategic advantage.

The use of legacy systems in an integrated ecosystem, a shortage of cyber talent, and a dearth of cybersecurity budgets propagate the risks and vulnerabilities faced by healthcare organizations (Coventry & Branley, 2018). Researchers called out the lack of funding for updating software security systems. Platsis (2019) highlights that 99% of all computer systems are vulnerable to threats. With the technological boom in healthcare, organizations are seeking to enhance the quality of healthcare; consequently, the medical domain suffers from technology-induced vulnerabilities and aftereffects. The SANS Institute proclaims that 94% of healthcare organizations have experienced a cybersecurity incident (Williams & Woodard, 2015).

Two competing requirements for cybersecurity in healthcare organizations are privacy and patient safety. Conventry and Branley (2018) advocated for cybersecurity to be a critical factor in the patient care culture that drives improved security and substantive processes. Human lives are at stake in healthcare organizations; hence, the need for cybersecurity resiliency and integrating cybersecurity into patient care culture. The other paralleling concern is attaining privacy standards to prevent identity theft. The healthcare industry suffers from repeated victimization of cyber-attacks, which resulted in the compromising of over 154,000,000 patients' records (Ronquillo, Winterholler, Cwikla, Szymanski, & Levy, 2018). Even with extensive regulations, the healthcare industry remains porous, vulnerable, and attractive to malicious cyber actors.

The purpose of this research is to call attention to the growing epidemic in the healthcare domain, which is not a disease but a cyber-attack. Given the sensitive and urgent medical operations occurring at healthcare facilities, the dire need for dynamic information security plans is imminent. The number of compromised health records lost my healthcare organizations is indicative of misaligned strategies, a thinning workforce, and determined adversarial and malicious cyber actors. Healthcare organizations can borrow security practices from other industries such as the financial, retail, and transportation to better (a) secure systems, (b) limit access to health records, and (c) encrypt data.

I will add more on privacy and human factors

References

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas*, *113*, 48-52

Davis, J. (2019, January). Healthcare cyberattacks cost $1.4 million on average in recovery. HealthITSecurity.com. Retrieved from https://healthitsecurity.com/news/healthcare-cyberattacks-cost-1.4-million-on-average-in-recovery

Haggerty, E. (2017). Healthcare and digital transformation. *Network Security*, (8), 7-11.

Karampela, M., Ouhbi, S., & Isomursu, M. (2018). Personal health data: A systematic mapping study. *International journal of medical informatics*, *118*, 86-98

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10.

Platsis, G. (2019). The human factor: Cyber security's greatest challenge. In *Cyber Law, Privacy and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1-19). IGI Global.

Ronquillo, J. G., Erik Winterholler, J., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA Open*, *1*(1), 15-19.

Stack, B. (2019, March 11). Here's how much your personal information is selling for on the dark web. Experian.com. Retrieved from https://www.experian.com/blogs/ask-experian/heres-how-muchyour-personal-information-is-selling-for-on-the-dark-web/

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices (Auckland, NZ)*, *8*, 305.