MO-ACHE Student Essay Award

An Administrator's Role in Healthcare Cybersecurity Management

Saint Louis University, May 2019.

Brenna B. O'Malley

brenna.omalley@slu.edu | (423) 464-3609

09/29/2017

Hospitals and other healthcare organizations (HCOs) are the front lines of healthcare and advanced medical treatment, but what happens when these places of safety and healing become a danger to customers' sensitive information and identity? In a time where technologies are advancing rapidly, and with them cybersecurity concerns, healthcare leaders around the world have great reason to be troubled by the negative effects of a potential data breach on their organizations. As identifiable patient data becomes increasingly more accessible through electronic health records and medical data is regularly uploaded to the cloud, it is now all too easy for this information to be stolen, and healthcare leaders must adequately prepare to protect against such attacks on patients' personal information or suffer an increased cost to their organization.

The 2017 Cyberthreat Defense Report surveyed over a thousand organizations across various industries around the globe and found that almost fifty percent of survey respondents estimated that their organization's network was successfully attacked between 1 and 5 times in the past 12 months. The majority of these breaches were likely due to poor employee security awareness as well as a shortage in information technology (IT) personnel (2017 Cyberthreat Defense Report, n.d.). Additionally, 45.0% of surveyed HCOs were affected by ransomware, a type of malicious software that withholds stolen data until the organization pays the ransom or employs personnel that are able to recover the stolen information without having to comply with the attackers' demands (2017 CDR, n.d.). Although the aforementioned statistics are troubling, they do provide some key areas for health administrators to focus on when trying to improve cybersecurity at their organization.

First and foremost, employees need to be effectively trained on cybersecurity threats and procedures, including the appropriate storing of data, the proper identification of phishing scams and malicious emails, and the use of work computers. In fact, 43% of healthcare breaches in 2016 were internal and included the loss of laptops and other devices that contained sensitive information (Barometer Breach Report, n.d.). These losses could have been managed by properly training staff on data security and by requiring any work-related technology to remain on-site in a secure location. To address these losses and improve cybersecurity in the healthcare industry, the Health Care Industry Cybersecurity Task Force (HCICTF) was established by the U.S. Department of Health and Human Services in 2016, and HCICTF identified cybersecurity training as one of its six high-level imperatives, ultimately recommending that cybersecurity education should be taught to all stakeholders in the organization, from executives to physicians to patients (U.S. Health Care Industry Cybersecurity Task Force, 2017). This is incredibly important because all employees are managing data in some fashion and are therefore responsible for safely and securely storing and using this information. An unfortunate click on a phishing email by an unaware administrator or physician can easily expose the entire organization to ransomware threats and can be avoided through proper cybersecurity training. By reinforcing the idea that all employees are stakeholders in the HCO's data security and by adequately training all employees on cybersecurity issues, health administrators can help decrease the likelihood of successful cyberattacks by creating a positive security culture.

It is important to keep in mind that effectively managing cyber threats does not mean that the number of threats will change in any way; the goal in improving an HCO’s cybersecurity is to decrease the number of successful data breaches and thereby decrease the costly risk of a damaging cyberattack. Expanding IT department staffing is a key way to manage these threats. The 2017 Cyberthreat Defense Report found that many IT departments are stressed and overwhelmed with the amount of information that they are required to process and manage due to understaffing and budget constraints. To improve the success of the IT department on cybersecurity measures and thus decrease the risk to the organization, appropriate expansions should be made by increasing personnel, budgets or both (2017 CDR, n.d.). On an administrative level, this should be considered an investment in the future of the HCO; as technology advances rapidly and becomes an integral part of the healthcare system, healthcare organizations and their IT departments need to adapt to match this increased need.

Overall, successful cyberattacks are becoming increasingly more common and are a significant cost to HCOs. In 2016 alone, there was an average of at least one successful health data breach every day, and over twenty-seven million patient records were exposed (Breach Barometer Report, n.d.). Considering the high probability and impact of a successful cyberattack, investment in proper employee education and the IT department are well worth the cost of implementing an adequate system. As technology becomes a major factor in the delivery and management of healthcare, cybersecurity should no longer be considered an IT problem as it is truly a concern for health administrators at all HCOs. With proper planning and education, health administrators can successfully manage these threats and improve the success of their organizations as a whole.

REFERENCES

CyberEdge Group. (n.d.). *2017 cyberthreat defense report.* Retrieved from http://www.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/Webroot_Q3_2017_CyberEdge_Cyberthreat_Defense_Report.pdf

Protenus, Inc. in collaboration with DataBreaches.net. (n.d.). *Breach barometer report: Year in review- 2016 averaged at least one health data breach per day, affecting more than 27M patient records.* Retrieved from https://cdn2.hubspot.net/hubfs/2331613/Breach_Barometer/2016/2016%20Year%20in%20Review/Protenus%20Breach%20Barometer-2016%20Year%20in%20Review-%20final%20version.pdf

U.S. Health Care Industry Cybersecurity Task Force (2017). *Report on improving cybersecurity in the health care industry.* Retrieved from https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014). Explaining users' security behaviors with the security belief model. *Journal of Organizational and End User Computing (JOEUC)*, *26*(3), 23-46. doi:10.4018/joeuc.2014070102