Journal of Radiology Nursing 38 (2019) 261–263

Contents lists available at ScienceDirect

Journal of Radiology Nursing

journal homepage: www.sciencedirect.com/journal/journal-of-radiology-nursing

Cybersmart: Protect the Patient, Protect the Data

Luanne Billingsley, DNP, MBA, APRN, ACNS-BC *

School of Nursing, Southeastern Louisiana University, Hammond, Louisiana

Keywords:
Cybersecurity
Nurses
Radiology

A B S T R A C T

The theme for recent national cybersecurity campaigns emphasized personal accountability and the importance of taking proactive steps to enhance cybersecurity. Personal and professional cyber lines blur as individuals become linked through the integration of the Internet of Things. The responsibility of health care providers to "protect the patient, protect the data" has become a 24/7 obligation. Interprofessional staff add to the challenge. Leadership teams should advance cybersecurity plans to meet the needs of areas such as radiology and support interprofessional education and training for the "connected nurse."

A number of national cybersecurity campaigns have emphasized personal accountability and the importance of taking proactive steps to enhance cybersecurity at home and in the workplace. Although October has been designated as National Cybersecurity Month, every month should be considered cybersecurity awareness month as the problem is omnipresent. A government and industry collaborative toolkit, with key messaging, articles, social media, and more, is available for individuals and organizations (Table 1). A glossary of relevant terms is provided for the reader in Table 2.

Cyberattacks are a multibillion-dollar disrupter of innovative technologies, used by the health care industry, specifically in areas such as radiology. Radiology departments have increased risk and vulnerability because of their complex, connected technologies, and workflow that includes accessing patient files from multiple systems, information requests, and placing examination orders from portable devices with varying levels of security. The more the access points in a network, the more the opportunities for hackers (Freiherr, 2017a,b; Jalali & Kaiser, 2018).

As the health care workforce becomes more interconnected in their personal lives through the broad Internet of Things' (IoTs) seamless technology, application integration through wearable devices, smart cars, and smart houses has blurred personal and professional cyber lines. All employees must be aware of how to secure their digital lives.

Cybersecurity: whose job is it?

Cybersecurity is everyone's business—many patients receive care from multidisciplinary clinicians and staff working in teams or as individuals. Everyone on the team must actively ensure patient safety and privacy.

One problem complicating successful cybersecurity results from the failure of health care agencies to properly integrate their IT function with the rest of the organization. That limitation perpetuates a lack of understanding by IT of the radiology department and a suboptimal understanding of cyber issues and procedures by the other departments. More mutual clarity would enhance the exchange of information and the effectiveness of privacy and security measures. This requires the involvement of stakeholders at all levels, administration leading, with an emphasis on changing the culture and attitude about the importance of cybersecurity.

Because of the interconnection of information systems, one person or department can adversely affect the entire organization's network. By understanding the complexity of radiology's clinical requirements, security programs can be improved to protect the entire organization (Zagoudis, 2017).

Nurses and other frontline staff can have a significant impact on cybersecurity at the point of care. Nurses collect and analyze relevant information to ensure that patients are receiving proper, timely, quality care. They are key members of the patient care team and should be significant contributors to the strategies of prevention, education, and recovery that every hospital can use to minimize damage from cyberattacks (Armstrong, 2019).

The radiology area is a complex data environment with many systems and entities where protected health information is

* Corresponding author: Luanne Billingsley, School of Nursing, Southeastern Louisiana University, Hammond, Louisiana.
E-mail address: Luanne.Billingsley@selu.edu.

https://doi.org/10.1016/j.jradnu.2019.09.010
1546-0843/$36.00/

Table 1
National cybersecurity awareness resources

Department of homeland security National cybersecurity awareness month 2019 toolkit	https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019

transmitted and stored, including radiology information systems, picture archiving and communication systems (PACS), computer information systems, digital imaging and communications in medicine (DICOM) files, imaging equipment, mobile devices, e-mails, short message service, cloud storage, patient portals, and revenue cycle management systems (Shindell, 2018).

Cyber risks

A unique set of data security challenges has arisen with the availability of ransomware and increased vulnerable targets provided by interconnected IoTs at home and in health care organizations. Examples include social engineering and phishing attacks aimed at individuals, attacks on credentials, network attacks, attacks via mobile devices and other wireless systems, interception of patient health information, alteration of records, and theft of storage devices. Studies have also shown that employees have the greatest vulnerability to cyberattacks resulting in data theft and malware-delivered ransomware attacks (Butler, 2018).

Numerous data pitfalls can be associated with radiology systems and workflow. Outdated equipment and software are weak points as they can be easily attacked by hackers to allow access to medical information systems. Manufacturers may no longer be providing security patches for operating systems, such as Microsoft NT and XP, leaving some devices such as PET and CT scanners, as well as infusion pumps, medical lasers, ventilators, and dialysis machines vulnerable to “medjacking” (Freiherr, 2017a,b). Legacy systems connected to PACS, which are connected to electronic medical records and best of breed systems that are installed as hospitals move to enterprise imaging, provide vulnerable points for hackers that seek unauthorized access to patient data for illicit financial gains and other motives (Freiherr, 2017a,b).

“Meaningful Use” mandates by the federal government have also created security issues around patient portals that are integrated with other information systems. When patients access patient portals via unsecured public networks, hackers can embed malware that could expose connected IT systems. Nurses and other health care workers can teach patients about the safe use of personal health information systems (Conaty-Buck, 2017).

Cost of cybercrime

The sale of patient records on the black market is profitable, yielding higher returns than credit card fraud. However, patient data do not need to be stolen to create problems. Information systems can be hacked, the data encrypted, followed by a demand for payment to restore access. According to the U.S. Department of Justice, this kind of attack called ransomware is the fastest growing malware threat from the home user to the corporate network. Malware is often delivered through “phishing” e-mails that appear legitimate or by visiting corrupted web sites. Since January 2016, over 4000 ransomware attacks have occurred daily, an increase of over 300% since 2015. Ransomware is a form of malware that targets data and systems leading to temporary or permanent loss of information, disruption to operations, financial losses, and potential harm to the organization's reputation. Civil damages of $1000 per patient in class action lawsuits can result, in addition to statutory penalties enforced by federal and state agencies. Data breaches can be significant. In 2016, the civil settlement of one case involving 6800 patients totaled 4.8 million dollars (Campbell, 2019).

The potential harm goes beyond financial cost. Networked medical devices like other computer systems include software with vulnerable access points. Cybercriminals can hack devices including MRI, fluoroscopy systems, and X-ray equipment affecting patient care. Hackers have even gained access via hospital WiFi networks (Freiherr, 2017a,b).

Cyber defenses

Effective prevention and response can mitigate the risk to the health care organization. Useful steps and information are shared in the “Protecting your Networks from Ransomware” guide (Table 3). Digital firewalls, detection software, and strong passwords, regularly updated, can be effective barriers (Storm, 2015).

No organization is immune to cyberattacks. Health care data losses can often stem from well-intentioned sharing as human users let hackers into an organization's systems. With breaches on the rise, nurses and other frontline providers with proper training can become the “human firewall” for their organizations to defend against unintentional sharing, unauthorized access, hacking, theft,

Table 2
Definitions

Term	Definition
Cyberattacks	A deliberate exploitation of computer systems, technology-dependent enterprises, and networks.
Cybersecurity	Preventative methods used to protect information from being stolen, compromised, or attacked.
Internet of Things	The network of physical objects embedded with electronics, software, sensors, and network connectivity that enables these objects to collect, store, and exchange data.
Malware	Shorthand term for malicious software and refers to any software that brings harm to a computer system.
Medjacking	The hijacking of biomedical devices to create backdoors in hospital networks.
Phishing	The fraudulent act of acquiring private and sensitive information, such as credit card numbers, personal identification, and account user names and passwords. Using web sites to lure e-mail recipients and Web users into believing that a spoofed web site is legitimate and genuine. Phishing is a social engineering technique.
Ransomware	A type of malware that infects, locks, or takes control of a system and demands a ransom to undo the restriction.
Social engineering	Nontechnical cracking of information security. The art of manipulating, influencing, or deceiving to gain control over a computer system. The hacker may use phone, e-mail, snail mail, or direct contact to gain illegal access. Social engineering attacks include phishing, spear phishing, CEO fraud, ransomware, and more.
Spear phishing	A variation of phishing directed toward groups of people. Spear phishing e-mails appear to come from a trusted source but are designed to help hackers obtain trade secrets or other classified information. A regular phishing attempt appears to come from a large financial institution or social networking site. In spear phishing, an e-mail appears to come from an organization that is closer to the target such as a particular company.

Adapted from Techopedia Dictionary (https://www.techopedia.com/dictionary).

Table 3
How to protect your networks from ransomware

How to protect your networks from ransomware technical guide	https://www.justice.gov/criminal-ccips/file/872771/download

and other losses. Organizations preparing to thwart cyberattacks must be willing to commit time, money, human resources and revise their technology, processes, and equipment as needed. A multilayered framework that includes functions provided by IT such as intrusion detection and prevention tools, end-point and mobile device protection, data encryption, patches and software updates, and other frontline defenses can be adopted and used by nurses (Billingsley & McKee, 2016). Beyond strong passwords, multifactor authentication (MFA) provides an additional layer of security. MFA can include facial recognition, fingerprint technology, and authentication applications (see Table 1).

Using a virtual local area network (VLAN) can limit access to equipment. VLAN functionalities can control access and limit communication with the main network. Antimalware can detect and quarantine threats in the system. Device users should be educated about necessary security procedures, including the use of personal mobile devices and USB thumb drives.

The organization should consider safety features before purchasing devices and make sure the manufacturer will provide continuing support. Organizations can request the Manufacturer Disclosure Statement for Medical Device Security (MDS2) form from the device manufacturer.

Cyber oversight: government agencies

The U.S. Department of Health and Human Services (HHS) has classified any ransomware attack to be a breach of patient data under HIPAA regulations. Such attacks also prompt notification to other federal or state agencies.

The three regulatory agencies that are responsible for regulating devices subject to cyberattacks are the Federal Drug Administration (FDA), the Securities and Exchange Commission (SEC), and the Health and Human Services Office for Civil Rights (OCR). Security and privacy of medical devices are regulated by the FDA, as recommended by the National Institute of Standards and Technology in its "Framework for Improving Critical Infrastructure Cybersecurity," which applies the following considerations: "identify, protect, detect, respond, and recover." HHS and OCR apply regulations under HIPAA, including transmission security, integrity controls, and encryption. Another federal agency charged with oversight regulations is the Federal Trade Commission which can apply sanctions for "unfair and deceptive practices" (Shindell, 2018).

Cyber education

Lack of awareness is a primary security issue in health care. Many businesses do not provide formal cybersecurity training. Therefore, employees may not realize the magnitude of risk associated with a cyberattack. The U.S. Department of Justice, charged with prosecuting violations, recommends training employees to recognize dangerous e-mails and operating system security holes, the use of strong passwords and spam filters, firewalls, updated software and firmware, and regular scans of drives and servers for viruses and malware. One breach can have significant consequences. A workable contingency plan must be in place to respond to an emergency of ransomware. This should be a part of the nurse's daily workflow and training.

Table 4
Cyber hygiene practices to protect employees and organizations

Never share passwords
Do not send private information over unencrypted mechanisms
Never disable antivirus programs
Do not download documents or files without permission
Do not open unexpected e-mail attachments
If hacking is suspected, appropriate staff should be notified immediately
Butler, 2018

To combat vulnerability to malware attacks, a study using simulated phishing revealed that almost one in seven simulated e-mails sent were clicked on by employees. Increased use of simulations was associated with decreased odds of clicking a phishing e-mail, suggesting a potential benefit of phishing simulation and awareness. Employee awareness and training represent essential components of protection against phishing attacks (Gordon, et al., 2019). Good cyber hygiene practices are recommended to protect employees and organizations (Table 4).

Conclusion

Five factors have been shown to adversely affect the development of cybersecurity in health care: a lack of resources, outside influences, organizational complexity, lack of corporate support, and cyber activity. Financial considerations can also be a significant factor as well as a lack of qualified staff, which may be outsourced.

The reality is that health care experiences more data breaches than any other industry with high rates of frequency, volume, impact, and cost. Cyberattacks can originate from anywhere. Cybersecurity is everyone's responsibility. Nurses, as connected persons are vulnerable to cyber disruption in the home and workplace. With proper training, nurses can become more secure by consistently practicing good cyber hygiene in their digital lives. Nurses have the knowledge and skills to be productive members of interprofessional cyber teams. As the largest segment of the workforce using information technologies across the organization, they can substantially contribute to protect patient data and improve patient safety. Nurses can be an effective frontline defense against cybercrimes.

References

Armstrong, J. (2018) How front-line caregivers can be prepared to blunt cyberattacks. Health Data Management. Retrieved from https://www.healthdatamanagement.com/opinion/how-nurses-can-stop-cyberattacks-and-hackers. Accessed September 3, 2019.

Billingsley, L., & McKee, S. (2016). Cybersecurity in the clinical setting: nurses' role in the expanding "internet of things. *Journal of Continuing Education in Nursing, 47*(8), 347-349.

Butler, S. (2018). Cybersecurity: why should we be concerned? *Journal of Radiology Nursing, 38*, 13-14.

Campbell, N. (2019). Managing to succeed: radiology's cybersecurity landscape. *Radiology Today, 19*(7), 8.

Conaty-Buck, S. (2017). Cybersecurity and healthcare records. *American Nurse Today, 9*(12), 62-65.

Freiherr, G. (2017a) The rising danger of cyber crime in healthcare. Imaging Technology News. Retrieved from https://www.itnonline.com/article/rising-danger-cyber-crime-healthcare. Accessed September 3, 2019.

Freiherr, G. (2017b) Agents of change: cybersecurity in a world of old and new. Imaging Technology News. Retrieved from https://www.itnonline.com/content. Accessed September 3, 2019.

Gordon, et al. (2019). Assessment of employee susceptibility to phishing attacks. *JAMA Network Open, 2*(3), e190393.

Jalali, M., & Kaiser, J. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of Medical Internet Research, 20*(5), e10059.

Shindell, R. (2018). Wearable devices: the next wave of Cybercrime. *Journal of AHIMA, 89*(3), 24-27.

Storm, D. (2015) Medjack: hackers hijacking medical devices to create backdoors in hospital networks. Computer World. Retrieved from https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html. Accessed September 3, 2019.

Zagoudis, J. (2017) *Building a Cybersecurity Team in Radiology* (pp. 1-6). Imaging Technology News. Retrieved from https://www.itnonline.com/article/building-cybersecurity-team-radiology. Accessed October 23, 2019.