Cybersecurity in the Healthcare Industry

It pays to be vigilant against potential attacks.

BY JULIE ANNE CHUA, PMP, CAP, CISSP, AND THE 405(D) TASK GROUP

This article is reprinted from Physician Leadership Journal, 2021, Volume 8, Issue 1, pages 23-2

Cyber-attacks on independent practitioners as well as large, integrated health systems have infected even the most protected networks. By the end of 2019, 764 healthcare providers had fallen victim to ransomware.[1] Phishing attacks increased throughout 2019; one aggressive phishing attack on the Oregon Department of Human Services system affected 645,000 patients.[2] The U.S. Department of Health and Human Services Office for Civil Rights Breach Report concluded that 38 million healthcare sector records were exposed in 2019 versus 7 million in 2018.

Recent highly publicized ransomware attacks on hospitals necessitated diverting patients to other hospitals and barred access to patient records, affecting care delivery. Such cyber-attacks can expose sensitive patient information and lead to substantial financial costs in an effort to regain control of hospital systems and patient data.

These attacks do not occur in a vacuum; they affect us all and continue to threaten sectors of our nation's critical infrastructure. There has never been a more critical time for our sector to address cybersecurity. Given the increasingly sophisticated and widespread nature of these attacks, the healthcare industry must make cybersecurity a priority and commit to the investments necessary to protect its patients.

Mobilization and Coordination

Similar to combating a deadly virus, battling cyber-attacks requires mobilization and coordination of resources across myriad public and private stakeholders, including hospitals, IT vendors, medical device manufacturers, and governments (state, local, tribal, territorial, and federal) to mitigate the risks and minimize the impacts of a cyber-attack.

Cybersecurity is an enterprise issue with consequences for the organization's mission, business, and programs—not just the IT department. For the healthcare industry, it is fundamentally about patient safety and uninterrupted care delivery. Not only is cybersecurity a challenge of technology and tactics, it also is a challenge of increasing awareness across all elements of healthcare organizations—doctors, nurses, administrators, healthcare practitioners, cybersecurity professionals, IT and non-IT experts, and engaging them in a mission that is about much more than technology.

Addressing this threat also requires a broad, collaborative approach across a multitude of organizations within the government and the private sector. The U.S. Department of Health and Human Services (HHS) is a dedicated partner in this mission and is working actively with a broad coalition of partners to enhance cybersecurity within the department and across the healthcare and public health sectors.

HHS uses a 360-degree view to ensure that cybersecurity efforts are based on a "one team, one fight" approach and continues to build partnerships with teammates in academia, medical research, and technology to become a better, more coordinated team.

HHS began this broad coalition

Continued on page 70

Cyber-attacks can expose sensitive patient information and lead to substantial financial costs in an effort to regain control of hospital systems and patient data.

Cybersecurity (from page 69)

approach in response to the Cybersecurity Act of 2015 (CSA). Under Section 405(d), Aligning Health Care Industry Security Approaches, HHS convened the CSA 405(d) Task Group to enhance cybersecurity and align industry approaches by developing a common set of voluntary, consensus-based, and industry-led cybersecurity

Continued on page 72

Five Current Threats

The five threats explored in the HICP document are as follows:

1 **Email Phishing**: Email phishing is an attempt to trick someone into giving out information using email. An inbound phishing email includes an active link or file (often a picture or graphic). The email appears to come from a legitimate source, such as a friend, co-worker, manager, company, or even the user's own email address. Clicking to open the link or file takes the user to a website that may solicit sensitive information or proactively infect the computer. Accessing the link or file may result in downloading malicious software or providing access to information stored on a computer or computers within the network.

2 **Ransomware:** Ransomware is a type of malware (malicious software) distinct from other malware in that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.

Hackers also may deploy ransomware that destroys or exfiltrates data, or ransomware in conjunction with other malware that does so. Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. Ransomware threats may incorporate tactics or techniques that are the same as or identical to other threats. For example, successful phishing attacks may lead to the installation of ransomware..

3 **Loss or Theft of Equipment or Data:** Every day, lost or stolen mobile devices such as laptops, tablets, smartphones, and USB/thumb drives end up in the hands of hackers. Theft of equipment and data is an ever-present and ongoing threat for all organizations. From January 1, 2018, to August 31, 2018, the Office for Civil Rights received reports of 192 theft cases affecting 2,041,668 individuals. Although the value of the device represents one loss, far greater are the consequences of losing a device that contains sensitive data. In cases where the lost device was not appropriately safeguarded or password protected, the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data.

4 **Insider, Accidental, or Intentional Data Loss:** Insider threats exist within every organization where employees, contractors, or other users access the organization's technology infrastructure, network, or databases. There are two types of insider threats: accidental and intentional.

An accidental insider threat is unintentional loss caused by honest mistakes, like trickery, procedural errors, or a degree of negligence. For example, being the victim of an email phishing attack is an accidental insider threat.

An intentional insider threat is malicious loss or theft caused by an employee, contractor, and other user of the organization's technology infrastructure, network, or databases, for personal gain or to inflict harm on the organization or another individual.

5 **Attacks Against Connected Medical Devices:** The Food and Drug Administration defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them; intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."

Consider this: Your practice is afflicted with a phishing attack that affects a file server that is connected to a heart monitor. While scanning the network for devices, the attacker takes control of all heart monitors in the ICU, putting multiple patients at risk. To learn more about the top five threats facing the healthcare industry and how you can mitigate them, check out the Health Industry Cybersecurity Practices Publication at www.phe.gov/405d. PM

Cybersecurity (from page 70)

curity guidelines, practices, methodologies, procedures, and processes that healthcare organizations can use.

To ensure a successful outcome and a collaborative public–private development process, HHS engaged a diverse group of healthcare and cybersecurity experts from the public and private sectors. Participation was open and voluntary. Out of this coalition, the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication was developed to raise awareness, provide vetted cybersecurity practices, and move organizations toward consistency in mitigating the most pertinent cybersecurity threats.

HICP Guidance

The HICP publication provides guidance on cost-effective methods that a range of healthcare organizations of every size and at every resource level can use to reduce cyber-security risks. Designed with everyone in the healthcare and public health sector in mind, the HICP document describes, at a high level, the current state of cybersecurity in the healthcare and public health sector and the top five threats we are facing. It sets forth a call to action for the healthcare industry, especially executive decision-makers, with the goal of raising general awareness of the issue. It also was developed to be read by doctors, nurses, administration officials, and any non-IT healthcare professionals who are seeking a background in the importance of protecting patients from cyber threats.

The publication includes a main document, two technical volumes, and a resources and templates appendix.

- The main document examines cybersecurity threats and vulnerabilities that affect the healthcare industry, including five current threats and 10 practices to mitigate those threats.
- Technical Volume 1 discusses these 10 cybersecurity practices for small healthcare organizations.
- Technical Volume 2 discusses these 10 cybersecurity practices for medium and large healthcare organizations.
- Resources and Templates includes a variety of cybersecurity resources and templates for end users to reference.

The technical volumes are designed with the IT department or IT contractor in mind and lay out the top 10 mitigation practices that should be implemented at every size organization to strengthen cybersecurity posture.

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication was developed to raise awareness, provide vetted cybersecurity practices, and move organizations toward consistency in mitigating the most pertinent cybersecurity threats.

405(d) Program Resources

In the past year, the 405(d) Program has extended its reach and continues to pursue its mission of aligning healthcare industry security approaches. The program can help many healthcare organizations with their cybersecurity needs, whether it's instituting a cybersecurity program structure using HICP or educating staff on cybersecurity. Following are the many different 405(d) programs and resources.

405(d) Awareness Materials. The 405(d) Program creates products that provide a rotating assortment of cybersecurity tips and best practices. Uniquely crafted cybersecurity awareness materials can be used as posters, email blasts, or print outs.

405(d) Guest Webinars. The 405(d) Program curates webinars specifically for organizations' cybersecurity needs and invites other federal partners where appropriate to help educate and inform the workforce on cybersecurity issues.

405(d) Social Media. The 405(d) Program is active on Instagram, Facebook, and Twitter at @ask405d. The social media accounts highlight new 405(d) awareness products and also provide cybersecurity best practices and tips that organizations can use.

405(d) Spotlight Webinar. Each 405(d) Spotlight Webinar highlights a new topic and task group member and focuses on how organizations have used the HICP publication, real-world scenarios and lessons learned, industry cybersecurity best practices, proven cybersecurity procedures and techniques, and other topics involving cybersecurity in the healthcare industry.

To receive any of these materials or calendar invites, email cisa405d@hhs.gov.

Conclusion

Over the past decade, the sophistication of cyber-attacks threatening the healthcare industry has increased dramatically and there are no signs that these threats will subside. Coming together and educating themselves is the best way the healthcare sector can establish, implement, and maintain current and effective cybersecurity practices.

In that light, HHS would like to leave physician leaders with a call to action: Stay engaged and active because this collaboration and coordination will thrive only if the sector stays engaged. **PM**

References

[1] Davis J. Cyber Threats Behind the Biggest Healthcare Data Breaches of 2019. Health IT Security. Jan. 3, 2020.

[2] Davis J. Breach Tally of Oregon DHS Phishing Attack Reaches 645K Patients. Health IT Security. June 20, 2019.

Ms. Chua is Risk Management Branch Chief, U.S. Department of Health and Human Services, Washington, DC.