Cybersecurity and Understanding Cyber Risk

Save to myBoK

By Diane Dolezel, EdD, RHIA, CHDA

Healthcare organizations are at risk for data breaches as the number of healthcare data breaches continues to rise annually despite efforts to slow the upward trend. Since 2009, there were over 2,000 data breaches reported to the Department of Health and Human Services (HHS).[1] Although only 18 data breaches were reported in the last three months of 2009, there were 271 breaches during the first nine months of 2018. To minimize cyber risk, organizations should scrutinize data breach reports and become informed about cyber risk threat vectors.

Data Breach Reporting

Healthcare data breaches are reported to the Department of Health and Human Services' Office for Civil Rights (OCR). The Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule states that, "A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information." Healthcare providers must notify HHS of breaches of unsecured personal health information affecting over 500 individuals, and they must notify affected individuals within 60 days of breach discovery. Under HIPAA, organizations must have user access controls to restrict employees' access to the minimum necessary information needed, and they must use physical access controls such as laptop cable locks, security cameras, regulated data disposal, and badge or biometrics access. The Health Information Technology for Economic and Clinical Health Act (HITECH) extends the breach notification rules to vendors and third-party service providers. As an illustration, a violation of the minimum necessary rule could occur if a message was left on a family member's home phone describing the patient's medical condition and treatment plan, when the patient had indicated that her work phone should be used for communications.

Examine Lessons Learned

Lessons learned from data breaches will drive cyber risk management because they identify threat vectors. Breaches are expensive on many levels. Breached organizations face damage to their reputation, digital disruption, clinical errors, litigation, and fines. Stolen patient information may be sold on the dark web, or utilized for digital extortion or phishing attacks.

In 2018, Anthem paid $16 million to HHS, the highest fine at the time, for a breach where a malicious email (phishing) attack hit a company subsidiary and provided passwords for downloading the protected health information of 79 million people.[2] A federal investigation revealed Anthem did not implement access controls, perform enterprise-wide risk analysis, or conduct adequate IT systems reviews.

Regarding lag time, in 2018 a Blue Cross Blue Shield employee error exposed healthcare data for three months, from April 23 to July 20, before being noticed.[3] These cases underscore the need for access controls, employee training, network monitoring, and data governance. Remember, if you can't measure your breach threat vectors and catalogue them in your risk management plan, then you can't harden your data defense perimeter.

Identifying Threat Vectors

Identifying threat vectors benefits risk planning. The ubiquitous usage of mobile devices, such as laptops and smartphones, exposes data to attack from malicious actors. Mobile devices are easy targets for data breaches. They are commonly used outside the facility over Wi-Fi networks and their security is often dependent on the users. Additionally, these devices may be lost or stolen, become infected with viruses, or be hacked. For mobile device management, the use of encryption, password protection, firewalls, remote wiping, scheduled software updates, risk assessments, and bring your own device (BYOD) programs are essential. Need incentive? MD Anderson Cancer Center paid $4.3 million for failing to secure and encrypt

patient's data, and Fresenius Medical Care North America paid $3.5 million for failing to conduct a complete risk analysis of their electronic protected health information.[4]

Medical devices present an attractive entry point for cyberattackers. A medical device is defined as "an instrument, apparatus, implement, machine, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals," according to the US Food and Drug Administration (FDA) definition.

Medical device manufacturers must adhere to FDA administration quality system regulations (QSR) on cybersecurity before and after they are approved for consumer use. The FDA collaborates with the Department of Homeland Security, medical device manufacturers, health delivery organizations (HDOs), medical researchers, and end users to secure medical devices.

For example, HDOs would work with the vendors to select a medical device, then the manufacturer would validate that any customizations (or future modifications) were compliant with the QSRs. Unfortunately, this system is lacking in checks and balances because the manufacturers self-validate with little technical oversight from the FDA.

A related concern occurs during vendor selection, when facility teams are challenged to perform security testing. For instance, can they tell if the vendor has a back door into the device's systems? To facilitate thorough security testing, many companies are contracting with security firms who perform cyberattack simulation testing.

HHS: What to Do Following a Cyberattack

The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) offers the following quick-response tips for HIPAA-covered entities to take in the event of a cyber-related incident.

In the event of a cyberattack or similar emergency, an entity:

- **Must execute its response and mitigation procedures and contingency plans.** For example, the entity should immediately fix any technical or other problems to stop the incident.
- **Should report the crime to other law enforcement agencies,** which may include state or local law enforcement, the Federal Bureau of Investigation, and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule.
- **Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs),** including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include protected health information.
- **Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals,** and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting.

Read the full recommendations at www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf.

Other Risk Vectors

Other risk vectors arise from databases, legacy systems, cloud storage, and business associates. Legacy systems are present at most companies, and many have software that cannot be updated. Moreover, their threat warning systems (if any) are not usually interoperable with the company's security monitoring systems, thus the legacy systems' warnings are not being passed to the security monitoring systems.

Regarding databases, an incorrectly configured Amazon data store caused Medcall Healthcare Advisors to breach personal data (emails, doctors notes, and Social Security numbers) of 10,000 consumers twice in one month during 2018.[5] As a suggestion, when reviewing potential threats from business associates or service providers think outside the box. Recall that these top companies have experienced cloud data breaches: Microsoft, Dropbox, Yahoo, Apple iCloud, and LinkedIn. Does your company or do your business associates use these companies' services? Do employees use them on company-owned

mobile devices? If you don't know the answers you may already be part of the collateral damage of these (or similar) commercial breaches.

Now is the time to be proactive, harden your cyberthreat defenses, and strengthen your cyber risk management plan. Consider this: when was your company's last cyberthreat drill? Clearly, hiring a security team should be a priority, and red team threat simulation drills are helpful.

Fortunately, there are many resources to guide these efforts. As a starting point, review the HIPAA crosswalk to the National Institute for Standards and Technology Cybersecurity Framework (National Institute of Standards and Technology 2014). Additionally, HHS has a cybersecurity checklist of steps to follow after a cyberattack and the Agency for Healthcare Research and Quality offers an information and privacy program.

Understanding Risk Lowers Vulnerability

The number of consumers affected by healthcare data breaches continues to rise annually despite efforts to slow the upward trend. Healthcare data breaches are costly on many levels. In the United States, the cost of cybercrime is estimated at $12.47 million dollars a year, and this will increase. Organizations need to identify cyber risk threat vectors, implement cyberdefenses, and manage problems related to cyberattacks.

Understanding cyber risk can help lower your cyberattack vulnerability. Healthcare data analysts will play a vital role in cyber risk mitigation, privacy and security education, and cybersecurity implementation. They could perform risk assessments, educate employees, supervise data governance, and run red team drills. Security managers and a strong security team should be part of an integrated security solution. Consider consulting with HIPAA experts to get a better handle on the relevant legislation.

Notes

1. McLeod, Alexander and Diane Dolezel. "Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches." *Decision Support Systems* 108 (April 2018): 57-68.
2. United States Department of Health and Human Services. "Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History." Press release. October 15, 2018. www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html?language=en.
3. Davis, Jessica. "Employee error exposed data of 16,000 Blue Cross patients online for 3 months." *Healthcare IT News*. September 21, 2018. www.healthcareitnews.com/news/employee-error-exposed-data-16000-blue-cross-patients-online-3-months.
4. United States Department of Health and Human Services. "Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules." February 1, 2018. www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/fmcna/index.html.
5. Davis, Jessica. "Update: Misconfigured database breaches thousands of MedCall Advisors patient files." *Healthcare IT News*. October 10, 2018. www.healthcareitnews.com/news/update-misconfigured-database-breaches-thousands-medcall-advisors-patient-files.

References

Agency for Healthcare Research and Quality. "AHRQ Information Security and Privacy Program." 2018. www.ahrq.gov/policy/electronic/privacy/infosecurity.html.

Carey, Susan. "Quest for Managing Cyberthreats in Healthcare." *Journal of AHIMA* 88, no. 5 (May 2017): 40-41,43. http://bok.ahima.org/doc?oid=302131.

Davis, Jessica. "1.4 million patient records breached in UnityPoint Health phishing attack." *Healthcare IT News*. July 31, 2018. www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack.

Davis, Jessica. "Phishing attack breaches 38,000 patient records at Legacy Health." *Healthcare IT News*. August 22, 2018. www.healthcareitnews.com/news/phishing-attack-breaches-38000-patient-records-legacy-health.

Department of Health and Human Services. "Breach Notification Rule." July 26, 2013. www.hhs.gov/hipaa/for-professionals/breach-notification/.

Department of Health and Human Services. "Breach Portal." https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Department of Health and Human Services. "Hospital Implements New Minimum Necessary Polices for Telephone Messages." www.hhs.gov/hipaa/for-professionals/complianceenforcement/examples/all-cases/index.html#case26.

Department of Health and Human Services and the National Institute of Standards and Technology. "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework." 2014. www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

Department of Health and Human Services Office for Civil Rights. "Considerations for Securing Electronic Media and Devices." Cyber Security Newsletter. August 2018. www.hhs.gov/sites/default/files/cybersecurity-newsletter-august-2018-device-and-media-controls.pdf.

Department of Health and Human Services Office for Civil Rights. "My entity just experienced a cyber-attack! What do we do now?" 2018. www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf.

Office of the National Coordinator for Health IT. "Top 10 Tips for Cybersecurity in Health Care." 2015. www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf.

Gibbs, David, Karima Lalani, and Alexander McLeod. "Beware the Internet's Dark Side: What HIM Professionals and Patients Should Know About the Dark Web." *Journal of AHIMA* 88, no. 8 (August 2017). http://bok.ahima.org/doc?oid=302209.

Lucci, Susan and Tom Walsh. "Cybersecurity 101." *Journal of AHIMA* 86 no. 11 (November 2015): 42-44. http://bok.ahima.org/doc?oid=107795.

McLeod, Alexander and Diane Dolezel. "Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches." *Decision Support Systems* 108 (April 2018): 57-68.

Ponemon Institute. "2017 Cost of a Cyber Crime Study." https://cdn2.hubspot.net/hubfs/85462/2018/2018_VUENUE/2018_BLACK%20HAT/Accenture-2017CostCybercrime-US-FINAL.pdf?t=1521831469946.

SANS Institute. "SEC564: Red Team Operations and Threat Emulation." 2018. www.sans.org/about/.

Diane Dolezel (dd30@txstate.edu) is an assistant professor, HIM department, at Texas State University.

Article citation:
Dolezel, Diane. "Cybersecurity and Understanding Cyber Risk." *Journal of AHIMA* 90, no. 4 (April 2019): 32-34.