COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 9. September 10, 2020 Updates, Asset Inventory Key to Countering Security Risks

By Jane Anderson

Government and health care industry experts recommend that health care organizations take a variety of steps, ranging from regular patching to better network access, to reduce their nonpandemic-related security risks.[1]

Beware of unsupported operating systems. The FBI warned specifically that systems running on Windows 7 are becoming a significant target for bad actors. But the FBI didn't limit its advice just to Windows 7: "Defending against cyber criminals requires a multilayered approach, including validation of current software employed on the computer network and validation of access controls and network configurations."[2]

The FBI encouraged organizations to:

- Upgrade operating systems to the latest supported version.
- Ensure antivirus, spam filters and firewalls are up to date, properly configured and secure.
- Audit network configurations and isolate computer systems that cannot be updated.
- Audit networks for systems using Remote Desktop Protocol (RDP), close unused RDP ports, apply two-factor authentication wherever possible, and log RDP login attempts.

Update your organization's disaster recovery plan. Rebecca Herold, president of SIMBUS360 and the CEO of The Privacy Professor, noted that the increase in work-from-home employees and telehealth workers due to the pandemic means the risk of disruption due to a natural disaster is greater than it was before the pandemic struck. She cited the derecho that knocked out power to one-third of Iowans; Hurricane Laura, which struck southwest Louisiana as a category 4 storm; and the wildfires plaguing western states.

These create "very real security threats to information," including the destruction of patient papers, digital files, and computer equipment, which may contain the only copies of data, Herold said. Updating disaster recovery plans, business continuity plans, and "backup plans and procedures must be done when work shifts from a secured facility to workers' homes and other locations, including onto employee-owned computers."

Create an IT asset inventory. In its summer cybersecurity advisory, the HHS Office for Civil Rights (OCR) reminded covered entities and business associates this summer that they need to ensure the confidentiality, integrity and availability of all electronic protected health information (ePHI) that they create, receive, maintain or transmit.

"However, despite this long-standing HIPAA requirement, OCR investigations frequently find that organizations lack sufficient understanding of where all the ePHI entrusted to their care is located," OCR said. "Although the Security Rule does not require it, creating and maintaining an up-to-date, information technology (IT) asset inventory could be a useful tool in assisting in the development of a comprehensive, enterprise-wide risk analysis, to help organizations understand all of the places that ePHI may be stored within their environment, and improve their HIPAA Security Rule compliance."[3]

Generally speaking, an enterprise-wide IT asset inventory is a comprehensive listing of an organization's IT assets with corresponding descriptive information, such as data regarding identification of the asset (e.g., vendor, asset type and asset name/number), version of the asset (e.g., application or operating system version), and asset assignment (e.g., the person accountable for the asset and the location of the asset), OCR said.

When creating an IT asset inventory, OCR recommended:

- Organizations should inventory hardware assets, including electronic devices and media, that make up an organization's network and systems. This can include mobile devices, servers, peripherals, workstations, removable media, firewalls and routers.
- Organizations should include software assets that run on an organization's electronic devices. Well-known software assets include anti-malware tools, operating systems, databases, email, administrative and financial records systems, and electronic medical/health record systems. "Though lesser known, there are other programs important to IT operations and security such as backup solutions, virtual machine managers/hypervisors, and other administrative tools that should be included in an organization's inventory," OCR said.
- Finally, organizations should tally data assets that include ePHI that an organization creates, receives, maintains or transmits on its network, electronic devices and media. "How ePHI is used and flows through an organization is important to consider as an organization conducts its risk analysis," OCR said.

"HIPAA covered entities and business associates are required to conduct an accurate and thorough assessment of the risks" to the ePHI they maintain, OCR said. "Identifying, assessing, and managing risk can be difficult, especially in organizations that have a large, complex technology footprint. Understanding one's environment—particularly how ePHI is created and enters an organization, how ePHI flows through an organization, and how ePHI leaves an organization—is crucial to understanding the risks ePHI is exposed to throughout one's organization."

Ignore basic security tenets at your own peril. John Ford, cyberstrategist for IronNet Cybersecurity Inc. and a former health care chief information security officer, said health care organizations have faced pandemic-specific challenges. For example, he noted an increase in remote access to electronic medical records systems, which can pose a security risk.

Ford recommended basic steps that can help to mitigate risks brought on by the pandemic and risks that are largely unrelated to COVID-19's effects on the health care system. At a minimum, he said, health care organizations should:

- Have complete knowledge of the computing assets of their organizations.
- Ensure those assets are patched, and implement updated security software.
- Enhance their ability to monitor network access.
- Update their auditing procedures given the changes to the operational environment and the restrictions on travel.

Contact Herold at rebeccaherold@rebeccaherold.com and Ford via Cara LaMaina at masessa@merrittgrp.com.

1 Jane Anderson, "Nonpandemic Security Risks Need Attention Now, Warn FBI, Experts," *Report on Patient Privacy* 20, no. 9 (September 2020).

2 FBI, "Computer Network Infrastructure Vulnerable to Windows 7 End of Life Status, Increasing Potential for Cyber Attacks," Privacy Industry Notification, August 3, 2020, https://bit.ly/3igf09W.
3 OCR, "Summer 2020 OCR Cybersecurity Newsletter: Making a List and Checking it Twice: HIPAA and IT Asset Inventories," HHS, last reviewed August 25, 2020, https://bit.ly/2R6P9W2.