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.