Codify by AAPC

Health Information Compliance Alert

Case Study: Manage Your Updates Accordingly to Close the Door on Hackers

You invite cyber threats in by mismanaging security and technology.

These days the slightest allowance lets hackers disrupt and take down even the most sophisticated networks. By assessing dangers and keeping abreast of suggested updates, you can save your practice a wealth of trouble.

Refresher: Data-for-ransom is the latest fad in the hacking world. Ransomware hackers breach servers, networks, and systems □ encrypting files containing documents and ePHI, then demand a ransom in exchange for the remedy needed to decrypt the files. And this type of malware (short for malicious software) causes mayhem, particularly for healthcare workers, who need precise data to safely care for patients.

Background: The healthcare industry, still quaking from the aftershocks of the WannaCry ransomware attack in May, was impacted again by a malware infiltration (Health Information Compliance Alert, Vol. 17, No. 6). "On June 27, 2017, NCCIC [National Cybersecurity and Communications Integration Center] was notified of Petya ransomware events occurring in multiple countries and affecting multiple sectors," said the **United States Computer Emergency Readiness Team (US-CERT)** in a July 1, 2017 release. "Petya ransomware encrypts the master boot records of infected Windows computers, making affected machines unusable."

Details: The Petya threat stemmed from similar problems encountered with the WannaCry attack, which included fallout from a missed Microsoft patch. Originating in the Ukraine, this newest ransomware iteration, has "wormlike spreading capabilities" and targets "Microsoft 7 machines," warned a **Microsoft Technet** blog post.

"The new Petya ransomware combines multiple well-known techniques for propagation and infection that are not new to security researchers," the Microsoft Technet blog post noted. "The noteworthy aspect is that Petya's developer(s) took techniques normally used by penetration testers and hackers, and built a sophisticated multi-threaded automation of these techniques inside a single piece of code."

Read the Microsoft Technet blog post at: https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/.

What Can You Do to Protect Yourself?

Both WannaCry and Petya were caused by missed updates. Some have suggested that cloud technologies and antivirus software could have halted the onslaught of the issues. But others warn that attacks like these are avoidable with proactive best practices. "Some of it's technical but the way that the attack comes into the network is deadpan simple," points out **Brand Barney, CISSP, HCISPP, QSA**, a security analyst with Security Metrics in Orem, Utah. "Some of these things are from pure neglect, which is really unfortunate."

Prepare: Hackers are resilient, but an attack is not inevitable. Health IT workers need to work in coordination with practice vendors to ensure compliance and security. "Cyber criminals prey upon the lax security practices, most breaches and attacks are preventable through a higher prioritization of operational security, including patch management and aggressive training programs," observes **Kurt J. Long,** founder and CEO of FairWarning, Inc in Clearwater, Florida.

Nuts and bolts: Network and technical security oversight leads to breaches □ it's just that simple. But you can protect your practice with HIT protocols. "Apply vendor recommendation patches aggressively, and watch for vendor updates vigilantly," suggests Long. "Not only should your IT team remain on top of such updates, but also, they should be driving a security-centric culture through your organization."

Long maintains that it should be a team effort and all staff must understand security compliance. "All team members should understand the importance of installing security updates and maintaining proper security protocols," he adds. "When everyone is on board, you can now plan and prevent for future attacks."

Are Small Providers Less Vulnerable to Hacking?

Many of these big-time ransomware attacks corrupt hospital systems on a massive scale, but don't be lulled into a false sense of security because your organization is small.

Reality: "Even small healthcare companies get hacked," warned **Thomas Lewis** in a blog posting for LBMC Security & Risk Services. "In fact, some hackers prefer smaller organizations because they understand that they can be easier targets."

And if a hacking incident leads to a HIPAA breach, the size of your organization won't protect you from a government audit and potential sanctions, Lewis cautioned. The HHS-OCR will investigate organizations of any size when they suffer a data breach.

Caveat: But the OCR does take into consideration your organization's size, as well as your budget and whether you have limited resources, Lewis noted. "As long as you've documented why you've made the choices you have, OCR will take this into consideration, but in all cases, you need to make sure you are meeting the HIPAA standards," he said.

Endnote: The HHS-OCR offers guidance, and small practices should take advantage of the plethora of federal information and assistance available to up their cybersecurity capital especially if they don't have the budget to invest in HIPAA and technological resources.

"Not all security measures require vast financial resources. Creating a culture of security where employees maintain a comprehensive understanding of cyber threats can help prevent cyber-attacks," Long advises. "From identifying and avoiding phishing attacks to the safe handling of customer or company data, team members can prove to be an invaluable asset to organizational security."

Resources: To take a look at the US-CERT report on Petya, visit https://www.us-cert.gov/ncas/alerts/TA17-181A.

To access the HIPAA Security Rule and HHS-OCR guidance, visit https://www.hhs.gov/hipaa/for-professionals/security/index.html.