Health Information Compliance Alert

Ransomware: Reduce Ransomware Hack Odds With This Expert Advice

Tip: Don't shirk on software updates.

A recent data security incident shows that even small practices are at risk of a ransomware attack.

Definition: Though data-for-ransom cyber attacks aren't as common as phishing in healthcare, they still happen to practices big and small. Ransomware hackers breach servers, networks, and systems - encrypting files containing documents and electronic protected health information (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.

Review This Case

Prospect, Connecticut optometrists, **Dr. DeLuca, Dr. Marciano & Associates, PC**, discovered their files had been encrypted and received a ransom request from hackers to release 23,500 patients' ePHI. The Nov. 29, 2018 attack "affected our network and some patient files by encrypting them," said the practice in an incident report.

After restoring the network with backup files, an investigation showed "that patient files containing personal information were stored on two servers infected by the ransomware. This information may have included patients' names, Social Security numbers, and limited treatment information," noted the brief. The practice immediately circumvented further attacks and upped its cybersecurity protocols by "closing all remote access to the network, installing enhanced antivirus software, and obtaining ransomware protection," the release explained.

Manage Your Patches

Luckily, the optometry practice had a plan in place that nipped the takedown in the bud. There are some steps you can take to cut down your chances of an attack before it happens while boosting your compliance protocols in the process.

Remember this type of hack doesn't discriminate. "Ransomware can affect practices through both targeted and non-targeted attacks," cautions **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with **Security Metrics** in Orem, Utah. "A lot of my customers think they're too small to be targets, and maybe that's true, but the non-targeted attacks are still out there."

Practices that ignore necessary software updates and installations leave the door open for hackers to step right in and infiltrate their systems. "The first two steps I recommend practices take to prevent ransomware are to make sure their antivirus and vulnerability patch management programs are in good shape," Stone advises.

Step 1: Sidestep malware issues with software that detects and prevents ransomware issues. "Antivirus [software] needs to be installed on all computers in the practice, configured to update automatically, perform both real-time and regularly scheduled scans, and not be able to be uninstalled except by administrators," stresses Stone.

Step 2: Keeping your software patches updated is critical to keeping predators out. "Vulnerability patch management is making sure operating systems and applications are regularly updated with security patches," Stone says. "One of the most common vulnerabilities I see with customers is that they either don't regularly patch their computers or, worse yet, they use older, unsupported operating systems, such as Windows XP, that can't be patched."

Comprehensive compliance planning helps manage your practice's risk of a ransomware attack, too. Annually assessing, then analyzing, and finally managing your risk helps you "determine which security controls to implement, based on the unique risks of the organization," Stone maintains.

Don't Let Lack of Compliance Funding Impede IT Security

The upkeep and implementation of a data security plan that includes HIPAA compliance can be costly, but pushing it to the last line item on your budget is a mistake. Sometimes cheap solutions lead to bigger headaches later on. Moreover, the price tag of a cyber incident usually far outweighs what you would have spent preparing your practice in the first place.

OCR worries: "For a long time, and still today, many compliance officers struggle to get the budget they need from upper management/executives to invest in their privacy and security program," observes attorney **Kathleen D. Kenney,** of **Polsinelli LLP** in Chicago. However, she maintains that investing upfront is essential and can be "night and day" if the HHS Office for Civil Rights should come knocking.

In addition, "cheap or free tools typically require more manual configuration and operation, so committing less budget to the tools could mean spending more on personnel to manage them," Stone warns. "Not having the security controls in place at all only saves money until the breach happens."

Tip: Training is key for small practices on a budget, indicates Stone. "For example, two common ways ransomware infects computers are through clicking on an infected email attachment and downloading malware from an infected website. If workforce members can be trained not to click on attachments and to stay away from all non-work-specific websites, the risk of being infected by ransomware will be lower."

Stone adds, "It would be even better if an email filter and the ability to block executables were implemented as well."

Reminder: Not only are there hidden costs after a data incident, like the loss of confidence your patients' have in safeguarding their ePHI, but there's the necessary security measures that must be implemented to eradicate the problem. And don't forget, there may be a significant fine to pay if your breach is determined a HIPAA violation.

Here's the maximum amount each HIPAA violation will cost you under the current civil monetary penalty (CMP) scales:

- $55,010 per HIPAA violation
- $1,650,300 annual cap
- The adjusted CMP is an increase from $50,000 per HIPAA violation with a past annual cap of $1,500,000.