Health Information Compliance Alert

Case Study: Watch Out For Sophisticated Malware Breaching Your Systems From Overseas

Pay attention: Massive breach teaches you four crucial lessons.

The latest HIPAA breach is the largest ever, affecting millions of patients across more than half of the United States. And this is the type of breach that strikes fear into the hearts of many healthcare providers find out why and what you can do right now to avoid the same disaster.

Background: Tennessee-based **Community Health Systems, Inc**. (CHS) has reported the breach of approximately 4.5 million patients' personal information, including patient names, addresses, Social Security numbers, telephone numbers and birthdates. The hackers accessed the patient records in the CHS system in April and June 2014. The affected patient population spans 28 states.

Keep in Mind HIPAA's Wide PHI Definition

"Although the breached records do not contain the details of the patients' treatment at CHS' hospitals, the identifying information in the records still meets the HIPAA definition of 'protected health information' [PHI]," noted attorney **Casey Moriarty** in an Aug. 19 **Ogden Murphy Wallace Attorneys** health law blog posting. "Therefore, CHS will have to follow the HIPAA breach notification requirements."

The hackers were an "Advanced Persistent Threat" Chinese group that used highly sophisticated malware and technology to attack CHS' systems, bypassing the security measures in place, reported partner attorney **Linn Foster Freedman** in an Aug. 22 privacy alert posting for the law firm **Nixon Peabody LLP**. Then, the hacker group copied and transferred the patient data outside CHS.

'Heartbleed' Bug Strikes Again?

"The technology is rumored to be the 'Heartbleed' bug," Freedman noted. Federal authorities identified the hacker group as typically seeking valuable intellectual property, such as medical device development data. But in this case, the group accessed non-medical patient data related to physician practice operations.

CHS first reported the breach to the **Securities and Exchange Commission** (SEC) and has hired the data security firm **Mandiant** to investigate the breach. CHS is also in the process of notifying the affected patients.

But because the data involved in the incident falls under HIPAA, CHS must also report the breach to the **HHS Office for Civil Rights** (OCR), pursuant to the Health Information for Technology and Clinical Health Act (HITECH), Freedman stated. And once CHS does so, this breach will become "the largest HIPAA breach reported to the OCR since HITECH was enacted in 2009."

Follow 4 Expert Tips to Prevent This Type of Breach

This type of massive, sophisticated data breach may seem impossible to prevent but you can actually avoid it by taking a few simple steps. Moriarty offered the following tips:

1. Safeguard & Educate: This large breach is yet another reminder to safeguard your electronic systems and educate your staff members on security policies and procedures.

2. Watch Staff Emails: The type of malware that caused this breach is relatively easy to overlook. A staff member who

clicks on a link in an email or responds to an email from hackers who pose as security personnel could result in unknowingly installing the malware.

3. Use Encryption: Consider employing encryption technology that meets the HIPAA breach safe-harbor standards to avoid or mitigate this type of breach.

4. Check with IT: When staff members are in doubt about a suspicious email, phone call or other communication, instruct them to always check with your information technology (IT) personnel and your HIPAA Privacy Officer before taking any action.

FBI: How Your IT Personnel Can Thwart This Attack

The threat of this type of breach is growing exponentially so much so in fact that the **Federal Bureau of Investigation** (FBI) recently released an alert. The alert states that the FBI has "observed malicious actors targeting healthcare related systems," possibly to obtain PHI or Personally Identifiable Information (PII).

"These actors have also been seen targeting multiple companies in the healthcare and medical device industry, typically targeting valuable intellectual property, such as medical device and equipment development data," the FBI warns. "Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware."

The FBI goes on to detail two main indicators of a possible compromise to your IT systems:

1. Network-Based Indicator. Outgoing traffic through standard HTTP/HTTPS ports 80, 443 (and possibly others), but obfuscates traffic by XORing the traffic with 0x36.

2. Host-Based Indicator. The malware runs as a Windows service "RasWmi (Remote Access Service)" from the malicious .dll C:\Windows\system32\wbem\raswmi.dll. The implant is installed from an executable file (the file has been observed under a variety of names) which drops the raswmi.dll file into the same directory and sets it to run as a service.