HealthCare
TRENDS

Follow us on

May 2016 *Issue II.*

Cyber-attacks in Healthcare: A Growing, Dangerous Concern

By William Ahrens | Senior Manager

For many years, the healthcare industry had been generally immune from the barrage of cyber-attacks which had been primarily directed towards the financial and retail sectors. In addition, data breaches tended to involve lost or stolen devices, often with unencrypted data.

No more.

Today, healthcare entities have become prime targets for cyber-attackers, who are drawn to rich repositories of personal data that can fetch prices 20 to 30 times higher on the black market than stolen credit cards. Last year, an estimated 66% of healthcare organizations experienced a cybersecurity incident impacting approximately 109 million patients.[i] Overall, cyberattacks cost the US healthcare system about $6 billion a year.[ii] The attacks often come from sophisticated networks of cybercriminals, often located overseas.

The potential damage to an institution's financial stability and reputation from one of these breaches is significant, which is why every executive along with members of the board of directors should be concerned. However, a 2015 survey of nearly 300 healthcare organizations found that just a quarter allocated more than 6% of their annual IT budgets to IT security. About half allocated less than 3%. In addition, few had committed a significant percentage of IT employees to the issue. [i]

Understanding the Breaches

While there are numerous types of attacks, including distributed denial of service, phishing, and advanced persistent threat attacks, healthcare executives should be aware of two recent additions:

- **Business email compromise.** Also known as "CEO fraud," this attack begins with an email sent directly to the CFO, ostensibly from the company's

CEO, asking for an electronic funds transfer. The email appears legitimate because it includes information gleaned from social media. The FBI issued an alert on this type of attack last year, calling it an "emerging global threat."

- **Ransomware**. Hospitals are the perfect target for ransomware, in which cyber-attackers infiltrate IT systems with malware. Once they have control of the system and/or its data, they demand payment to return control. In February, Hollywood Presbyterian Medical Center experienced a ransomware attack that prevented staff from being able to access electronic health records. The hospital eventually paid hackers $17,000 in ransom to regain access. A similar attack at MedStar Health in Maryland required the system to shut down its entire computer networks for several days and providers to revert to paper processes.

"...Not only can hackers then move into the organization's main IT systems from the device, but they could reprogram them to cause harm to patients."

Connected Devices a Threat

Hackers have a unique advantage in hacking into hospital systems that doesn't exist in either retail or banking sectors: interconnected medical devices. Nearly every device in a healthcare setting, from infusion pumps to MRIs, has a computer chip that allows it to communicate with the EHR and other systems. Most run legacy software that hasn't been updated in years and have hard-wired passwords that haven't been changed. Not only can hackers then move into the organization's main IT systems from the device, but they could reprogram them to cause harm to patients.

Taking an Offensive Approach

It is nearly impossible to completely protect your IT systems against cyberattacks. However, there are numerous steps healthcare organizations can take to minimize the number and severity of such attacks:

- Employ a strong security posture, including multi-layered endpoint and network security, encryption, strong authentication and monitoring capabilities; first-and-foremost, ensure all software and plug-ins are up-to-date.
- Regularly conduct risk assessments and mock exercises; analyze the results, assess lessons learned, and quickly address any identified vulnerabilities.
- Provide mandatory ongoing education and training for all employees; enforce the use of strong passwords; in addition, make sure users understand and practice good security hygiene.
- Hire and maintain an appropriately sized and skilled IT security team. Also consider pre-contracting with top-tier managed security service providers and third-party experts to assist in the event of a breach.

It's not a question of whether or not your facility will be attacked; it will, and probably already has. The question is: "Can I contain the damage and defeat the attackers?"

For more information contact:

William Ahrens| Senior Manager
212.375.6662
William.Ahrens@WeiserMazars.com

Visit us on **www.weisermazars.com**

[i] HIMSS. *2015 HIMSS Cybersecurity Survey.* 2016. http://cynergistek.com/cynergistek-resources/himss-cybersecurity-survey-results/.

[ii] Pettypiece S. Rising Cyber Attacks Costing Health System $6 Billion Annually. *Bloomberg Technology.* May 7, 2015. http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually. Accessed April 21, 2016.

Disclaimer of Liability
Our firm provides the information in this e-newsletter for general guidance only, and does not constitute the provision of legal advice, tax advice, accounting services, investment advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation.

***WeiserMazars LLP** is an independent member firm of Mazars Group.*

***CONFIDENTIALITY NOTICE:** The information contained in this communication may be privileged, confidential and protected from use and disclosure. If you are not the intended recipient, or responsible for delivering this message to the intended recipient, you are hereby notified that any review, disclosure, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender immediately by replying to the message and deleting it from your computer. Thank you for your cooperation. WeiserMazars LLP*