How the healthcare industry can fight rising cyber-attacks

By Jason G. Weiss

The healthcare industry is facing an alarming proliferation of cyber perils. Hospitals and other facilities and healthcare-related businesses are under cyberattack 24 hours a day, seven days a week, 365 days a year. Why? Because our healthcare system is a "soft target," and particularly vulnerable because of its lifesaving work, where time is of the essence. It's a recipe for disaster from a cybersecurity standpoint.

The dangers to the healthcare system are clear in the statistics. According to the *Journal of the American Medical Association*, in 2018, the number of annual healthcare data breaches surged 70% over the previous seven years. In 2017 alone, there were over 500 healthcare-industry data breaches, leading to the loss of over 15 million patient records. The start of 2019 has even been worse. Healthitsecurity.com estimates that in just the first six months of this year, over 25 million patient records have been breached and stolen.

And hacking isn't the worst danger. Even greater threats come from ransomware, malware and new types of disruptionware attacks. The healthcare industry is the number one victim of ransomware attacks, with approximately 35% of all ransomware attacks leveled at healthcare sectors. These attacks have devastating effects on healthcare operations, infrastructure usage and patient care. The attacks are also disastrous from a financial standpoint. In 2018, over $8 billion was paid in ransomware damages. Over $3 billion of that amount was paid out to cyber criminals to try to recover encrypted patient data.

Cyber-criminals have also fashioned another cyber threat: medical device hijacking, or "medjacking." In 2015, the FBI believed medjacking to be such a hazard that it referred to the hijacking of medical devices as a "ticking time bomb" and issued a warning to the healthcare industry. Today, there are legitimate worries from the World Economic Forum that medjacking attacks could come from not only a cyber-criminal hacker but from terrorist groups and even rogue nation-states.

The security weaknesses of medical devices are similar to those of the Internet of Things. Many of the devices were built on older or unsecure operating systems, in an era of manufacturing where cyber-security was not considered as important as it is now. Security was so weak that hackers could use infected e-mails, or malware on memory sticks, to take control of lifesaving machines. Moreover, if hackers could gain access to a single medical device in a healthcare system network, they could possibly access all of the linked devices. The medical providers were, for many years, not even aware of the depth of this threat. A recent study found that, on average, U.S. companies took 206 days to even detect a data breach in their networks.

The damage has, ironically, been triggered, in part, by passage of the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH Act). The Act incentivized medical professionals to convert patient medical records into Electronic Health Records, or "EHRs." In fact, since 2011, 84% of all hospital emergency departments exclusively use EHRs, exposing hundreds of millions of patient records to cyber theft.

Fighting Back

The healthcare industry and regulators have taken steps to fight back, but much more needs to be done. There has been little improvement in addressing cybersecurity vulnerabilities in the medical device industry. Many devices work using wireless internet technology, which until recently relied on security that generally could be overcome in a matter of minutes. While wireless technology defense is slowly improving, it is still a relatively easy for even moderately skilled hackers to infiltrate wireless devices, even when a device is actually inside a patient. In one high-profile example of the risk of this threat, the United States Secret Service required former Vice President Cheney to remove the wireless functions of his heart defibrillator to protect him from the risk of a cyber-assassination attack.

Now, researchers are examining dozens of medical devices for security flaws, and have found serious cyber-security weaknesses in many devices, such as infusion pumps, used to inject medication directly into the bloodstream of patients. Deadly vulnerabilities were also found in dozens of other devices, according to weforum.org, including X-ray systems, CT scanners, medical refrigerators and implantable defibrillators. The FDA has expressed concern about the need to improve security, but these devices are still being sold, as they are critical for treatment.

One way healthcare providers are trying to safely store, maintain and back up personal health information (PHI) is through cloud storage. Over 83% of healthcare organizations in 2019 are using cloud services, and that number is likely to increase due to the requirements of the GDPR, the CCPA and HIPAA.

Many believe that cloud services better protect patient data than "brick and mortar" facilities, where it is difficult to trace medical or patient records that "walk out" the door. Additional benefits of cloud computing include large data storage capabilities, scalability of service, better HIPAA compliance, and the availability and control of medical and patient data, to name a few. Cloud services such as Microsoft, Google and Amazon devote substantial resources to protecting their cloud data from cyber-criminals.

Still, cloud security is not by any means foolproof. There are vulnerabilities of successful "phishing" attacks as well as the constant concern about "insider threats."

Phishing and "spear phishing" techniques are among the most effective methods of spreading ransomware and malware. Phishing is the fraudulent practice of sending an email pretending to be a reputable person or company in order to induce individuals to reveal certain information or to release malware, ransomware or some other cyber malady on an internal computer network. A study by *Proofpoint* showed a 300% jump in phishing emails directed at the healthcare industry between the first quarter of 2018 and the first quarter of 2019.

Insider threats are also a major source of damage. They can potentially access the healthcare cloud through physical internal healthcare networks, minimizing many of the security features cloud computing can provide. In a *Forbes* 2018 study, 58% of healthcare breaches involved "inside actors." Many are motived by financial gain: stolen patient data can be used to commit identity theft, tax fraud and credit fraud, to name just a few crimes thriving under the weight of patient data theft.

How to keep safe?

IT vigilance and employee awareness training are two key ways the healthcare industry can combat these burdensome, expensive and possibly life-threatening cyberattacks.

The healthcare industry should view improving IT defense as a major aspect of its overall cyber defense posture. Better hardware, better application whitelisting and better overall network security are critical to control the flow of PHI information whether the data is stored "in house" or in the cloud.

The problem is compounded by new laws like the California Consumer Privacy Act which create a "private right of action" for data breached or stolen from any provider, healthcare included. If a healthcare system is breached, the cost could become astronomical based on statutory damages these new privacy statutes.

Finally, it is critical for the healthcare industry to offer effective employee cybersecurity awareness training to prepare them for the cyber threats facing them today.

Most ransomware, malware and disruptionware can be deflected if an employee does not fall for simple phishing schemes. In one instance, a cyber-criminal spread flash-drives in a business parking lot; an employee took one of the drives into the office and unwittingly unleashed malware into the company's network.

Cybersecurity awareness training is one of the most important and reasonably low-cost approaches to cyber defense. If an employee knows what to do, and more importantly what **not** to do when cyber challenges arise, it could save the company not only lost dollars but more importantly it may protect, preserve and secure critical company data.

Finally, the Department of Health and Human Services (HHS) has recently issued Cyber Security Guidance Materials, which include a cyber-security checklist and a cyber-security infographic. These materials can be found at hhs.gov and include cyber-awareness newsletters and a section on dealing with ransomware.

It's clear that the healthcare industry is under attack by cyber-criminals, both within the United States and around the world. Hacking, ransomware, malware, medjacking and cloud computing security all present a multitude of issues for the healthcare industry to confront in 2020 and beyond. By taking action, such as aggressive IT vigilance and employee awareness training, the industry can better protect against these threats. ■

Jason G. Weiss *is Counsel in Faegre Drinker, Biddle and Reath's Information Governance and E-Discovery group, where his practice focuses on cybersecurity preparedness and response, and compliance with CCPA and other information governance laws. Prior to joining Faegre Drinker, he was a Supervisory Special Agent in the FBI Los Angeles Cyber and Forensics branch, where he founded, designed, and lead a nationally-recognized and accredited computer forensics laboratory.*