COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 1. January 31, 2018 Outlook 2018: Use Training, Patching to Counter More Sophisticated Cyberthreats

By HCCA Staff

Expect more phishing, more ransomware and more cyberattacks using the internet-of-things in 2018, as hackers use increasingly sophisticated tools and techniques to steal and sell valuable medical records or to deny health care entities access to their own systems for ransom money.

Humans remain the weakest link in the security chain, security experts tell *RPP* in a series of interviews, and organizations' HIPAA security personnel should focus on training to ward off threats in 2018. They also need to focus on their business associates to make certain they are also complying. Neglected patches for known security vulnerabilities and poor security in internet-of-things devices also represent growing threats, experts say.

David Harlow, principal in the health care law and consulting firm The Harlow Group LLC, anticipates similar attacks to what was seen in 2017. "Most hackers rely on a combination of technical vulnerabilities that are exacerbated by human factors," Harlow tells *RPP*. "For example, the largest breach of the past year, the Equifax hack, was made possible by the failure of staff to apply a patch released by a software vendor to address a known vulnerability."

Phishing and ransomware attacks will continue to exploit humans, who are "the weakest link in our cybersecurity infrastructure," Harlow says. "The coming year is likely to bring new and different versions of the same-old, same-old—the hackers are becoming more and more sophisticated, spoofing URLs, for example, in a manner that is entirely indistinguishable from the real thing by anyone but the most sophisticated users."

Roger Shindell, president and CEO of Carosh Compliance Solutions, tells *RPP* that 2018 will see an increase in ransomware. The health care industry will continue to see more of a threat than other industries due to the value of medical information on the black market, he says.

Hackers Will Exploit Same Vulnerabilities

Hackers have been successful employing ransomware and exploiting unpatched systems, and so they'll continue to do so in 2018, says Patricia Shea, partner at K&L Gates LLP. "After all, why mess with success?" she tells *RPP*. "I expect more sophisticated phishing, ransomware, and opportunities to do bad things because of the exploding array of devices and connectivity and data. There are just so many entry points."

Bad actors will ramp up their profiling of potential victims based on internet activity and other online information available to them, Shea says, and will be able to create scenarios that are plausible and non-suspicious. In addition, the "bring your own device" problem will continue, she says. "Health care entities need to take a long, hard look at their policies and procedures for permitting these devices to be used and whether the risk is simply too great," she says. "If they permit it, they must require safeguards such as encryption to be installed. The potential for misuse—intentional and negligent—is very real with the use of these devices."

Tareva Palmer, chief information security officer at WVU Medicine, says the types of threats health care entities experience in 2018 will be the same as those seen in 2017. "External bad actors are always a concern, attempting

to gain access for monetary gain from stolen medical and financial information. This includes identity theft and medical fraud as well as ongoing malware threats. Threat vectors such as phishing attempts and network scans aimed to detect exploitable vulnerabilities continue to be on our radar," she says.

Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor, says she expects the most significant threats in 2018 to include:

◆ increases in ransomware and associated ransom costs;

◆ increases in denial of service attacks, particularly through internet-of-things devices;

◆ increases in insiders selling patient data, since insiders realize that data is valuable;

◆ more breaches from lack of training and awareness, especially since organizations are providing less training, not more; and

◆ more and larger breaches from business associates who "simply still do not think they need to comply with HIPAA."

Shindell also cites security lapses at business associates as an under-addressed security problem, although he says the problem is getting some awareness and is attracting attention from OCR: "Expect this to become a growing trend in 2018."