HCCA
HEALTH CARE
COMPLIANCE
ASSOCIATION

Compliance TODAY

June 2016

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Using technical safeguards to thwart phishing attacks

an interview with Adam Greene

Partner, Davis Wright Tremaine

See page 16

23
Who's minding the store? Understanding supervision requirements
Maryann C. Palmeter

32
Compliance in a new, value-based care world
Daniel Esquibel, Ryan Haggerty, and Peter A. Khoury

39
What is the "right" observation rate
Ronald L. Hirsch

45
Quality cancer registry data: How accurate is your data?
Candice Morrison-General

Adam H. Greene, JD, MPH
Partner, Davis Wright Tremaine
Washington, DC

an interview by Adam Turteltaub, CHC, CCEP

Meet Adam Greene

*This interview with **Adam Greene** (AdamGreene@dwt.com) was conducted by HCCA/SCCE Vice President of Membership Development **Adam Turteltaub** (adam.turteltaub@corporatecompliance.org) in February 2016.*

AT: You're a nationally-recognized authority on HIPAA and the HITECH Act, and you primarily counsel healthcare systems and technology companies on compliance with the HIPAA privacy, security, and breach notification requirements. Cyber security is among the top risk areas compliance and ethics professionals are concerned about in 2016. So please tell us what is the difference between "cyber security" and "information security"?

AG: There is not always consensus, but I consider cyber security to be a subset of information security concerning the Internet. For example, a thief stealing a laptop is an information security matter, but arguably not a cyber security matter. A hacker accessing your network or even remotely taking control of an insulin pump is a cyber security issue.

AT: Do hackers and other cyber criminals represent a significant risk to healthcare entities? Why would they want health information?

AG: 2015 represented the year that health information clearly became a top target for cyber criminals. A few hacking cases in 2015 impacted over 100 million individuals, more than all large breaches in previous years combined. The problem may have been around for some time before 2015, but last year was when healthcare organizations started to discover these breaches.

We seem to be seeing two main reasons why cyber criminals want health information. The first is identity theft and other types of fraud. Health information is often particularly rich data, providing everything a criminal potentially needs to commit identity theft. Accordingly, anecdotal reports indicate that the street value of a health record is much higher than, for example, a credit card number. Credit cards can expire or get deactivated, but health information is often data (such as date of birth and Social Security number) that cannot be changed. The second reason seems to be the collection of background information, potentially for purposes of intelligence gathering. For example, some of the largest 2015 breaches are purportedly traced to China and efforts to collect intelligence on large volumes of people (although China vehemently denies such claims).

Health information is often particularly rich data, providing everything a criminal potentially needs to commit identity theft.

AT: What types of cyber threats should healthcare entities be worried about?

AG: Ransomware is becoming a growing threat. This is where someone encrypts the victim's computers and will not provide the key unless paid. Even when an organization has an up-to-date backup, removing the malware and restoring the systems can be a lengthy process that can significantly disrupt all of the organization's operations. If the organization does not have a backup or the backup is corrupted (possibly by the attacker), then patient data may be irretrievably lost unless the ransom is paid. This has become enough of an issue that HHS put out an alert on it at the end of January. The alert proved quite timely, as a string of hospitals across the country have since been victims of high-profile ransomware attacks, with potentially many more attacks going unreported.

Phishing continues to be a growing concern. Some of the largest 2015 breaches have been traced back to successful phishing attacks, where a user within the healthcare entity clicks on a link in a fake email, leading to a malware infection that potentially infects the network.

Some of the more exotic threats involve medical devices. Hackers have demonstrated that they can remotely take control of medical devices. This has been portrayed in popular entertainment, such as a "Homeland" episode where a hacker kills someone by remotely controlling their implanted pacemaker. In reality, the threat is real, but it is hard to say if the risk is significant, because the likelihood may be so small. But you can imagine the consequences if this type of cyber attack was used by a country in the midst of a war.

AT: Because so many of the attacks involve tricking employees into relinquishing information, it argues strongly for teaching employees to be more vigilant. What are some specifics that you think employees should be taught?

AG: One place to start is focusing on phishing attacks. Phishing refers to a hacker sending a fake email to try to infiltrate systems. Employees clicking on links or attachments in phishing emails have led to some of our largest breaches. Organizations should consider providing training using real phishing attempts to demonstrate that modern phishing emails are not filled with spelling and grammar mistakes.

And organizations should consider regular phishing exercises by sending fake phishing emails and providing additional training to anyone who clicks on the link or attachment. They can also provide rewards to users who properly detect and report phishing attempts.

Another place to focus is password management and the dangers of sharing passwords across systems. Organizations should consider whether they are willing to permit and support the use of password management, because it is easy to tell an employee to maintain a different password for every system, but it is unrealistic to expect that they will do so and use strong passwords without password management software or similar tools.

> But, while organizations can create all the policies that they want, they must be realistic that there will always be some employees who do not follow them.

Third, organizations can emphasize that passwords should never be communicated with anyone, including IT. Sometimes, IT needs to be reminded of this. Otherwise, hackers can obtain access to a system by posing as IT.

At the end of the day, however, employee education will only get you so far. No matter how much training you do, some employees are going to fall for a phishing attempt or social engineering attempt. Accordingly, organizations should also be focusing on what technical safeguards they can put in place so that if a hacker gets into information systems, the damage can be contained.

AT: Part of the problem is that the criminals are getting really good at what they do. They can make it look like an email is coming from an employee's boss. Is it time for us to start making policies that certain requests need to be confirmed over the phone or face to face?

AG: It's not a bad idea. I think it's something for each organization to consider. At a minimum, organizations should train employees to be suspicious of an email coming from a boss or other person of authority that requests data in an unusual fashion. For example, if an email comes out of the blue requesting a file with sensitive information, then a verification call would be entirely appropriate. But, while organizations can create all the policies that they want, they must be realistic that there will always be some employees who do not follow them. Accordingly, there must be good technical safeguards to protect against human error.

AT: Law enforcement has been encouraging companies to come forward sooner, rather than later, when they detect an incident. What's your sense of when organizations that are victims of an attack should reach out to law enforcement for help?

AG: I agree that it's best to bring in law enforcement pretty early on. It is always important to first activate the incident response plan, bring in the right people, and get to work on forensic analysis. For example, it may be best to have forensic imaging done before calling law enforcement. But once the initial steps are done, an early decision should be contacting law enforcement. Law enforcement may be able to shed additional light on the situation, based on what they are seeing elsewhere, and a slow response with involving law enforcement could be second guessed later during litigation.

AT: Thank you for sharing your insights.