From 28 years with the FBI to solo compliance consultant

an interview with Charles E. Colitre
Compliance and Privacy Officer, Crystal Clinic Orthopaedic Center

See page 18

29
Prescription drug copayment coupons come under OIG scrutiny
Hannah Levinson

33
Provider-based facilities and compliance trends
Zorana Vojnovic

39
OIG 2015 Work Plan, Part 2: Do fewer projects mean a sharper focus?
Nathaniel Lacktman

47
Compliance professional 2.0: Soft skills needed
Tom Fox

This article, published in Compliance Today, appears here with permission from the Health Care Compliance Association. Call HCCA at 888-580-8373 with reprint requests.
Hackers have an unspoken code: The easier to crack, the better. They’re out to get the lowest hanging fruit, and most refuse to climb up a ladder to snag fruit just out of reach. Healthcare entities, especially small to midsize, are right at eye level and have lots of juicy protected health information (PHI) waiting to be plucked.

So how do you move this fruit out of reach?

First, let’s learn about our enemy
Healthcare entities account for the highest percent of all US data breaches,\(^1\) so, it only makes sense that compromising healthcare would be a fast and easy way to gain valuable data to make a profit on the black market.

Thanks to the Internet, supreme intelligence isn’t required to be a hacker. Most stand on the shoulders of their hacking world superiors, and use pre-made tools to steal data from vulnerable organizations. One such tool is the Windows-based point-of-sale malware package Backoff,\(^2,3\) which created quite a buzz in September 2014 and became an epidemic striking hundreds of entities.

Most hackers pry their way into healthcare networks by exploiting known weaknesses (also known as vulnerabilities) in computer code and applications that allow them to bypass many security measures. The problem in healthcare is that important aspects of IT security are sometimes left hanging, and vulnerabilities are left wide open.

What is the best course of action for those in healthcare looking to secure their patient environment? Learn how to find and fix those vulnerabilities to make sure environments are as out of reach from hackers as possible. The following are five recommendations on creating an inhospitable environment for hackers.

Vulnerability scanning
Vulnerability scans are automatic tests that run on software, hardware, and network structures. Their goal is to find vulnerabilities, and some can find more than 50,000 unique vulnerabilities. (That’s 50,000 different ways a hacker could get into your system!)

The most important part of a vulnerability scan is remediation. Once a scan completes, you (or your IT department) must fix any vulnerabilities immediately on a prioritized basis. The longer vulnerabilities are left open,
the more of a chance they could be exploited by criminals.

The average hacker can skim the entire Internet for potential victims once every hour. That means as soon as you attach a system to the Internet, the system is being probed... unless you have implemented a solid firewall.

After you’ve fixed everything, security best practice is to immediately run a vulnerability scan again, just to triple check that no problems remain. Your remediation efforts may not have been enough, or for all you know, new vulnerabilities might have popped up today as you were remediating yesterday’s vulnerabilities. As you can probably deduce, vulnerability scanning is not so much an event as an ongoing process that should happen at least quarterly, if not monthly.

Two-factor remote access
LogMeIn. RemotePC. pcAnywhere. GoToMyPC. Any of those sound familiar? If they do, that probably means someone at your organization uses remote access to gain admission to your patient database. Do you use a third party for IT support or billing? Odds are you allow them to access your network through remote access too.

Here’s the bad news. Remote access is one of the most insecure applications used by organizations today, and may allow attackers to gain direct access to your patient data. This doesn’t mean you shouldn’t use remote access, but it does mean you should take the steps to secure it.

The most secure way to use remote access is through two-factor authentication, which is exactly what it sounds like, a two-step process. Two different forms of authentication are necessary to access an application.

When setting up two-factor authentication, factors must contain two of three aspects:

1. Something only the user knows (e.g., a username and password)
2. Something only the user has (e.g., a cell phone or RSA token)
3. Something unique to the user (e.g., a fingerprint)

Factor 1 could be a user name and password. Factor 2 could be a four-digit PIN sent through an SMS to your phone. An attacker would have to learn your username/password and have your cell phone to gain access. But that’s just one example. There are many different combinations of two-factor authentication, such as USB tokens, fingerprints, smartcards, or patterns.

Proper segmentation
A key security component in any organizational environment is proper network segmentation, which simply means that parts of a network are separated from others with no or very limited connectivity between them. In healthcare’s case, the parts with patient data should be separated (or segmented) from everything else.

When an environment has no segmentation, it’s called a flat network. Many businesses use flat networks because they are extremely simple to understand and build. However, if an environment contains sensitive information, such as PHI or credit card information, flat networks bring extreme liability.

An easy way to limit your exposure to hackers is to segment your network so patient data and the systems that process, transmit, and store it are isolated from all other network processes (like browsing the Internet, etc.) Network segmentation is usually provided by an industry-standard firewall. Depending on the complexity of your environment, segmenting your network can be quite difficult.
Wireless security
According to a 2013 Software Advice survey,5 60% of patients say free Wi-Fi would somewhat minimize their frustration with doctors’ office delays. And that’s great if your network is set up correctly.

Just like oil and water don’t mix, neither should your workforce wireless network and patient wireless network. In addition to different wireless networks for workforce members and patients (e.g., DrBrown and DrBrownGuest), it’s imperative to ensure both networks are actually separated by a firewall. If not, you could be putting your organization in serious jeopardy. You could allow impermissible disclosure of patient data and not even know it.

When you set up your network, the little acronym next to the security encryption standard you choose will be a crucial part of your security. Is it WEP, WPA, or WPA2? Or do you have an open wireless network with no encryption at all? Best practice for Wi-Fi security is to use WPA2 encryption. WPA and WEP encryption are outdated and easily cracked.6

As you set up WPA2 for both your guest and non-guest wireless networks, make sure the password you use is secure. Do not use the default password or username that comes with your wireless router!

Here are some great password criteria that apply to the creation of a Wi-Fi password, and also any other password in your work environment:

- Eight characters (for patient Wi-Fi)
- 14 characters+ (for workforce Wi-Fi)
- Uppercase letters
- Lowercase letters
- Numbers
- Special characters

Thorough risk analysis
A good risk analysis sets the tone for your organization’s security. Because it identifies and defines the parts of your environment that touch patient data, it can also identify vulnerabilities in those crucial areas.

Vulnerabilities common in healthcare environments found via a risk analysis can be digital, physical, internal, external, negligent, or willful. For example:

- IT personnel leaving a virtual backdoor into an environment for easy access in the future
- Business associate using insecure cloud services to store patient information (Did you know more than 90% of cloud services in healthcare pose a medium-to-high security risk?)
- Lack of physical barriers in the front office to protect access to patient data
- Workforce members forgetting to lock computer screens when they leave their desk

Remember...
Security is an ongoing process, not an event. Even if you were 100% secure today, vulnerabilities will spring up tomorrow that could increase your risk and make you vulnerable to a data breach. The more often you update your systems, check for vulnerabilities, and consult your IT/Security department or vendor, the higher up the tree you place your fruit to avoid the hacker’s greedy (but lazy) hands.

References: