Protecting health data in a troubling time

Understand who and what you're up against.

By Ron Ropp and Becky Quammen

"The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won't suffice. Even with oversight, the policies and procedures may not be effective: My access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully."

— Kevin Mitnick, infamous convicted computer hacker, in a statement delivered to the Senate Committee on Homeland Security and Government Affairs in 2000, just six weeks after his release from prison.

This observation from Kevin Mitnick, a hacker who, according to his own testimony, has "gained access to some of the largest corporations on the planet, and … successfully penetrated some of the most resilient computer systems ever developed," is one that healthcare leaders need to take to heart in quick order. Why? It looks as if healthcare organizations are losing the war on data protection to the bad guys, and therefore need to quickly find a way to turn things around.

Indeed, large-scale healthcare data breaches are becoming alarmingly commonplace, according to a research letter published in the April 14, 2015, issue of the *Journal of the American Medical Association*. In fact, from 2010 to 2013, nearly 1,000 large breaches affected more than 29 million individual health records, and more than half resulted from theft or loss of laptops, thumb drives, and paper records, according to the report, which is based on researchers' evaluations of government data. The yearly number of breaches rose from 214 in 2010 to 236 in 2011, 234 in 2012, and 265 in 2013.

What's even more disconcerting is the fact that hacking incidents more than doubled during those years, according to the U.S. Department of Health and Human Services database of breaches of unencrypted health information, which includes information reported by Health Insurance Portability and Accountability Act (HIPAA) covered entities.

"We found that as many as 30 million records were compromised in a four-year span," said lead author Dr. Vincent Liu of the Kaiser Permanente Division of Research. "If each of these represented records from a unique patient, it could suggest that as many as one of every 11 American's healthcare data has been compromised."

So far, in 2015, large-scale data breaches have continued to plague the industry. Perhaps most notably, a breach at Anthem Health affected about 80 million people and is being described as the largest healthcare data breach ever. According to a news release from the healthcare payer, hackers "gained unauthorized access to Anthem's IT system" and obtained personal information from current and former members, such as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses, and employment information, including income data.

As a result, business leaders cannot assume that they are immune from cyberattacks and data breaches, and must start to think – and act – more strategically to protect their healthcare organizations' data.

Reading their minds

To start, as a healthcare leader, you need to understand how the bad guys think and use that understanding to protect your organization. The "check the box" mentality of performing security assessments is no longer enough and can simply mask problems. Instead of just thinking of what security measures you can take, you need to form a proactive defense that takes into account the fact that these bad guys are likely to do the following:

- Walk through a parking lot and randomly check for unlocked car doors;
- Circle around a building and check dumpsters in an effort to find discarded paperwork;
- Walk in a delivery entrance and see how far they can get before being stopped;
- Peruse your websites and social media pages and download all the documents and videos for tidbits of information;
- Collate the names of your employees and providers so they can gather their schedules (and announced vacations on social media);
- Compile the names of all newborns born at your facility;
- Call and act like a provider or employee to have their password reset;
- Volunteer at your healthcare facility to gain access;
- Act (and dress) like a delivery service or vendor to gain access to your facility;
- Infect/sniff or capture wireless network traffic while sitting in the lobby or parking lot; and/or
- Hack the Facebook, Twitter, or other online accounts of your employees.

In essence, the enemies in these scenarios will look for the easy ways to gain access to data. More often than not, they won't take the difficult road – breaking through your firewall or kicking in the front door. Instead, they will find the unlocked door, the un-configured Web application, the recently terminated employee account, the unprotected community outreach portal, the unintended information shared on social media, or data stored on commercial services – or, they will simply steal your laptop from the back seat of your car while you are grabbing lunch.

Unfortunately, healthcare organizations across the country figuratively leave the back window open on computer systems while barring the front door more often than most will admit. Remember, a misconfigured or incomplete system or application that is put into production without testing, or an unfinished project, or lack of change control on day-to-day operations are apt to leave your organization exposed.

Hackers are not going to announce their arrival and try to scale the walls on your systems. They are going to find the "hidden" employee entrance and let themselves in, get what they want, prop a few other windows and doors open, then let themselves back out without you ever knowing. Many times these exploits sit unnoticed. Having systems, processes, and software that are proactive rather than reactive is good, but everyone in your organization also needs to change their mindset by getting into the minds of the enemy – and thinking like a bad guy when protecting systems, software, and people.

It is especially imperative for you, as a healthcare leader, to have a mindset that considers things you might think as outlandish to protect your organization. You cannot stop every threat, but you can make sure you are not leaving yourself open to easy access. Thinking like the bad guy is a great way to start a data-protection initiative.

In parts two and three of this ongoing series, we will look at how you can build upon this philosophy and further protect data at your organization by understanding your own vulnerabilities and then creating a comprehensive strategic plan that will help to safeguard patient information. **HMT**

Ron Ropp, Chief Technology and Security Officer, **Quammen Health Care Consultants**

Becky Quammen, CEO, **Quammen Health Care Consultants**

Reprinted from July 2015

Health Management TECHNOLOGY™
The Source for Healthcare Information Systems Solutions www.healthmgttech.com