THINKSTOCK

NOT IF, BUT WHEN

Healthcare may seem to have been unscarred by the ongoing rash of high-profile cyber-attacks, at least compared with retail and financial organizations. But to hear security pros tell it, the industry is increasingly finding itself as much of a target as companies in other sectors—if not more of one. **Karen Epper Hoffman** surveys the potential damage

Given all the rules designed to protect medical information (even from family members), individuals might reasonably believe that data held by healthcare providers are invulnerable to theft or other violation. To that assumption, healthcare experts say: Uh, not so much.

While retailers and financial institutions are often seen as being in the crosshairs of the hacking community, it is the healthcare industry that is increasingly under siege by cybercriminals looking to access valued information and data assets. According to a report released last year by the Ponemon Institute, attacks on healthcare data systems doubled between 2010 and 2014. Data breaches cost healthcare organizations $5.6 billion annually; nine out of ten respondents to the Ponemon survey said they had suffered at least one breach in the last two years.

"There's a general perception, and I don't think it's accurate, that commercial retailers have more records compromised in any given incident," says Christopher Paidhrin, former chief information security officer of PeaceHealth Medical Group and current information security manager for the City of Portland, Oregon. "I think that commercial retail is just much better about getting the message out."

In Paidhrin's experience, healthcare organizations have less mature security controls and practices than the retail and financial sectors, which similarly hold valuable personal and financial information. Indeed, a 2014 BitSight Insights report found that healthcare entities respond more slowly to security violations, with the average online compromise lasting roughly 5.3 days. Unlike financial services companies, which are built to detect fraud and quickly act to shut down compromised accounts, physicians, hospitals and insurance companies are not as fast to detect, flag and block illegitimate access.

Until recently, regulation surrounding breach reporting was a lot less stringent for healthcare providers than for financial services firms. "And the smaller [healthcare] providers and community hospitals and private medical practices are even further behind," adds Bruce Forman, chief information security officer for UMass Memorial Health Care. "Because there haven't been a lot of breaches reported, it's assumed that healthcare is ahead of the game."

While Forman believes that more healthcare providers are encrypting employees' laptops and mobile devices, he says that it remains "hard to figure out the data that might have gone missing and what was on the devices … [There are] not enough [security] people watching the store and not enough technology to see attacks coming."

A hospital might spend hundreds of thousands of dollars on a new CT scanner or an MRI machine but struggle to justify spending a fraction of that on security software to protect records.

Big data, big value

As Forman and Paidhrin note, the value of healthcare records is actually much greater than personal information that might be gleaned from an attack on a financial services company or a retailer. Stolen medical information—which, in addition to health records, includes diagnosis codes, billing data and insurance information—could be used to order medical equipment or drugs—even to create fake identities.

Stolen healthcare records, in fact, can fetch 10 times the sum of a stolen credit-card number on the black market. Too, once stolen, private healthcare information can often be resold multiple times without the pilfering organization noticing for weeks or months. "This gives cyber-thieves a huge incentive to target healthcare," Paidhrin says. "The lifecycle of a stolen payment card number is measured in days. A medical record lasts a lifetime."

At the same time, the proliferation of healthcare data—especially as organizations share access with various insurers, partners and third-party vendors—has increased the potential attack vector for data thieves, according to Jon Wilkinson, privacy officer for Philips Healthcare. Then there's the expanded use of mobile technologies and cloud computing, which can create additional IT security vulnerabilities. "With all these integrated new systems … the vulnerability increased simply because there are more vendors to be managed," Wilkinson explains. "Vendor management is often treated as an item on a checklist, rather than something subject to careful audits."

Given the implementation of new payment technologies and the consistently high value of healthcare data on the black market, it's hardly surprising to read big-picture assessments like the one delivered in Experian's 2015 Data Breach Industry Forecast: "Several factors suggest the healthcare industry will be plagued with data breach headlines … The expanding number of access points to Protected Health Information (PHI) and other sensitive data via electronic medical records and the growing popularity of wearable technology make the healthcare industry a vulnerable and attractive target for cybercriminals."

Still, as Paidhrin points out, the technology that healthcare organizations utilize for patient care, record keeping and data analysis often far outpaces the technology used to secure data assets. "Healthcare IT security maturity is really challenged," he says. "These organizations have a long history of purchasing the greatest technologies but not [investing in] the security to protect them."

In other words, a hospital might spend hundreds of thousands of dollars on a new CT scanner or an MRI machine but struggle to justify spending a fraction of that on security software to protect records and networks. With so many hospitals using legacy devices or equipment that was designed without security in mind, Paidhrin says that "there's nothing to stop an attacker from plugging into the network and sniffing whatever is traveling the network." Even more ominously, that doesn't account for the plethora of unpatched or unmanaged applications. At the hospital where he works, Paidhrin says there were 360 managed applications in use, but more than 700 unmanaged ones.

Forman says that much of the problem lies with healthcare organizations' reliance on the same controls they have used for years—like traditional antivirus protection, which scans for specific signatures and not the behaviors that more advanced security technologies track. "This was something most of us didn't need to worry about five years ago, when everything was relatively segmented," he explains. Wilkinson agrees, adding, "Legacy systems are not being given the same level of care and concern as the newer systems … [They] need to be retired appropriately."

Information security officers are typically aware of these issues. But, here again, many healthcare organizations lag their peers in other sectors even when it comes to employing a dedicated IT security chief, according to Forman. He says the job of overseeing information protection often gets split between a number of managers, none of whom count data security as a top priority.

Next steps

In the face of this snowballing security crisis, what can healthcare entities do to better protect data assets? Locking down support from the C suite is a good first step, according to Paidhrin.

"Having an executive leader or a board member as a champion for the information security program is key," he says. "Then you have a representative who understands that while the patient's health is the organization's aim, it also needs to preserve and protect their information." This individual can play a pivotal role in ensuring that budgetary resources are earmarked for security.

Paidhrin also underscores the importance of peer networking among security chiefs in healthcare, which leads to sharing information about ongoing breaches, new security technologies and threat information. "The security community is very collaborative," he notes.

Wilkinson highlights the need for healthcare organizations to scrutinize their business associates' security as well as their own – in essence, to make sure that security is being "properly managed all the way down the chain." Forman recommends that healthcare companies tap a trusted third party for regular security assessments, during which that party might attempt to poke holes in existing systems and help develop an overarching security strategy.

"People want a magic bullet," Wilkinson says. "But really, the goal should be to identify [attacks] in days or hours, rather than weeks or months." ■