Cybersecurity

Avoid and address common security mistakes

Staying on top of security can seem like an impossible task, especially when basics such as password security still have the power to baffle organizations. But complex threats such as phishing and sophisticated malware attacks are coming fast and furious these days. Knowing where to put resources can be difficult.

Experts agree that each organization has unique security vulnerabilities and must craft a security program that meets its individual needs. However, there are some common vulnerabilities and mistakes that organizations should pay particular attention to.

Taking security seriously

One of the biggest mistakes organizations make is the assumption that simply checking off items on the HIPAA compliance checklist translates into a meaningful and effective security program, says **Kevin Beaver, CISSP,** independent information security consultant with Principle Logic, LLC, in Atlanta.

"This mindset and approach is pervasive in the healthcare industry, from the smallest of clinics to the largest of hospitals and insurance companies, and it's why so many organizations keep experiencing negative security events," he says.

When security is simply a compliance requirement that isn't translated into a core value for the organization, it won't get the needed investment from leadership and participation from staff. Security isn't just the job of

the security officer; everyone at an organization must be part of its defense, especially leadership. Security is a core business function, and not acknowledging that at the highest levels of management is one of the top security mistakes in the industry, Beaver says.

Following policy

Organizations sometimes rely too much on security policies to prevent incidents and breaches, Beaver says. Ineffective policies that simply satisfy compliance documentation requirements don't necessarily address underlying issues.

"Not unlike how we rely on pills to fix many of our health problems, the root causes of security issues go way beyond any documentation," Beaver says. "The core issues need to be treated rather than covering things up, addressing the symptoms. Policies don't get hacked; vulnerable systems and gullible people do."

Some organizations don't bother to implement or enforce the policies they create, Beaver adds. That's another common mistake, and one that can turn out to be particularly costly in the event of a breach. Policies that aren't followed are more of a liability than a defense and can punch holes in an organization's defense strategies during audits, he says. In April, OCR announced a $2.5 million breach settlement with CardioNet, a Malvern, Pennsylvania–based organization that provides remote cardiac monitoring services. One of the findings OCR cited in its report was that CardioNet's security policies and procedures were only in draft form and were not implemented.

And that wasn't a one-off incident. In February, OCR reached a $5.5 million settlement with Memorial Healthcare Systems (MHS) in Hollywood, Florida, for a breach that affected 80,000 individuals. MHS employees snooped in patient records using the login credentials of a former employee of an affiliated physician office. MHS had workforce access policies and procedures in place but didn't implement them. User access wasn't reviewed, modified, or terminated, and MHS did not audit activity logs. To make matters worse, MHS itself identified these risks in several risk analyses conducted between 2007 and 2012.

Patches and updates

Patch management turned out to be especially critical this year, but poor patch management remains another common security mistake, Beaver says. In May and June, WannaCry and NotPetya hit organizations around the world. But evading the attack was as simple as running a currently supported operating system or installing emergency patches released in March for legacy operating systems. Putting off patches and, in particular, ignoring third-party software updates are common mistakes, Beaver says.

"These are the flaws that are targeted and successfully exploited via malware and hacking tools more than practically any other security attack method," he says.

Routine training

Organizations are required to train staff on HIPAA, which includes the requirements of the Security Rule and the organization's security program. Many organizations assume that the same old training they've used for years is good enough, Beaver says. Although routine training can work for some staff and is a good way to introduce security to new hires, he says, organizations need to move away from the concept of static, repetitive training and work to actively engage staff and build knowledge.

"It might help provide an initial layer of defense, but it's certainly not everything most people in charge of security and compliance make it out to be," Beaver says. "It has to be measured, tweaked, and made interesting to keep people engaged over time."

Training shouldn't be a one-size-fits-all system, says **Ben Goodman, CRISC,** founder and CEO of 4A Security and Compliance in New York. Organizations should include information on current threats and create role-specific tips for recognizing and thwarting them, he adds.

"Phishing exercises need to be part of that training as well," Goodman says. "It's one of the most common tactics; it happens to employees at all levels in the organization all the time."

Backing up

A backup can be a lifesaver in the event of a major security incident such as a ransomware attack. If an organization's system is corrupted or damaged beyond recovery, it can restore from the most recent, uncompromised backup—provided the backup system is working.

Backing up data is critical, but the data and the backup process itself must be regularly reviewed and monitored, Goodman says. Many organizations have backups and have been running them for years—but without anyone actually testing them, he says. This can lead to unpleasant surprises when the test is finally run.

"They test them and it turns out it hasn't worked for seven months," Goodman says. "It's just not something they think about. It's set up and it runs, and then something changes and it doesn't work anymore."

All too often, it's only when a crisis strikes that an organization discovers its backups repeatedly failed, he adds.

Data management

Another common mistake is poor data asset management, Beaver says. Too many organizations don't know what information is where and what risks the information is currently exposed to.

"You absolutely, positively cannot secure PHI or other important information assets that you don't acknowledge," he warns.

Creating a reliable inventory of data assets sounds simple, yet it's a pervasive problem, Goodman says. Organizations should regularly inventory all their data assets, including mobile devices, medical devices, and systems and assets set up in remote offices or schools.

"The main risk is actually one of these devices that's not encrypted getting stolen," Goodman says. "Simple as that."

Once all data assets are identified and inventoried, ensure they're encrypted, Goodman says. Encrypting a device is an easy fix for a major vulnerability.

"Encryption is another thing that is very important and in most cases not that terribly difficult or expensive to accomplish," Goodman says. "That's one that we commonly see organizations haven't gotten around to doing, and yet it's one of the best ways to secure the data."

Networking

Network configuration is an area where many organizations make mistakes, says **Larry Ponemon, CIPP,** founder and chairman of the Ponemon Institute in Traverse City, Michigan. Organizations often use a flat network, he says—one large, unsegmented network in which all systems, devices, and applications are connected. Flat networks can be easier to maintain and administer, but they're not suitable for most healthcare organizations. They can cause traffic issues and, most importantly, they leave an organization vulnerable to a massive breach, Ponemon says.

"If, for example, everything is relatively secure but there's one application that isn't, that vulnerability can get into everything," he says.

The interconnectivity offered by a flat network can be useful for some functions, Ponemon says. It's easier to run reports and analyze workflows on a flat network, but an organization must be aware that this configuration comes with a risk.

"There's a real business reason for doing it that way, but it makes the data susceptible to leakage," he says.

A hierarchal network, on the other hand, implements network segmentation and layers of security, Ponemon says. Although a hierarchal network might take more resources to maintain, it can keep a security incident from spreading throughout the system.

Bare minimum

HIPAA establishes a basic floor for security standards. Although some organizations might believe that merely meeting the requirements is sufficient, in today's increasingly complex cybersecurity environment, the bare minimum won't cut it. Simply checking off compliance requirements doesn't mean an organization is truly secure. And, although paying a HIPAA

violation settlement fine can cost an organization several million dollars, it's not necessarily the biggest breach cost. Breach notification costs and recovery costs can take a huge bite out of an organization's revenue. See the November 2016 issue of **BOH** for more on the costs of a security breach.

Yet the assumption that compliance equals security is one of the biggest mistakes organizations make, Beaver says.

HIPAA provides a place for organizations to start, but protecting PHI—and sensitive business information—requires organizations to take a more active stance. The Health Care Industry Cybersecurity Task Force released a report in June detailing the security vulnerabilities facing the industry and recommended ways to address them. Although some of the recommendations require cooperation from government agencies and vendors, the report discussed a number of no- or low-cost fixes organizations can implement themselves, such as adopting the National Institute of Standards and Technology's cybersecurity framework. For more on the report, see the August and September issues of **BOH.**

Organizations need to look at data such as PHI as valuable—OCR certainly does, Ponemon says. Even beyond HIPAA, other state and federal regulations can kick in when an organization experiences a data breach. What's more, corrupted or missing medical records could impact reimbursement. In an increasingly knowledge-based economy, data truly is important.

Addressing common security mistakes can seem like a difficult task. Many of them are systemic issues that require all parties to work together to make change. But, it's not impossible, Beaver says. Leadership, a security- and privacy-focused culture, and most importantly discipline can help organizations overcome common security mistakes, he says.