Protecting Labs Against Cyber Threats

FIVE EXPERT TIPS

1. **Keeping systems up to date and free of any vulnerabilities** is at the top of the list to avoid security breaches, but is easier said than done. It requires constant monitoring of connected devices, operating systems, and programs for updates, patches, as well as unnecessary files or users.

2. **Enabling two-factor authentication** is something that comes up repeatedly in conversations about cybersecurity, and many hospitals have already jumped on board. But some smaller organizations still need to catch up. Two-factor authentication requires something in addition to a PIN or password to access data, such as a physical card or badge, or a user’s voice or fingerprint.

3. **Setting up your system to be able to manage isolated breaches** is one way to avoid downtime in patient care. “You have to build processes into the design so that a single point of failure won’t result in downtime,” said David Robb, manager of laboratory information systems at Sutter Health in Palo Alto, California.

4. **Training end users is essential**, according to David Finn, the healthcare IT officer of Symantec. He suggested training lab workers who may not regularly interact with IT about what to look out for and how to alert IT about problems that could indicate security breaches. “End user training is the biggest bang for your buck when it comes to cybersecurity,” he said.

5. **When it comes to buying new lab equipment**, choosing devices carefully also goes a long way, Robb noted. Red flags include vendors who use out-of-date software themselves, or vendors that rarely issue patches for security holes. “When you pick instruments, you should pick them as a package with redundancy and the operating system in mind,” Robb said.

Technology (IT) department seem like a hassle—the threat of hackers breaching laboratory information systems is a real and growing one, according to experts.

“If you connect to the internet, you’re not safe,” said David Finn, the healthcare IT officer of Symantec, a large enterprise cybersecurity company. “So the belief that your systems are safe because you operate in a rural area, or you don’t have celebrity patients, or your facility is not an academic institution just isn’t true.”

Imagine the consequences if all your lab’s data—past and present—were posted in the public realm. Consider what would happen to the flow of patient care if you couldn’t access your lab’s computers or databases for days on end. “If a lab gets shut down, you’ve now impacted all the operations of a hospital,” Finn said. “Obviously there are patient care consequences in that.”

However, that worst-case scenario is often avoidable. By being aware of cybersecurity best practices, taking steps to protect data, and having back-up plans in place, laboratories can fend off cybersecurity threats.

A Treasure Trove for Hackers

Historically, hackers looking to infiltrate databases of personal information have pursued the networks of banks and credit card companies. But, thanks to better security tactics by those industries over the past decade, many hackers are starting to shift their focus.

“Healthcare hasn’t been as robust in its security as other industries,” said Marti Arvin, the vice president of audit strategy at CynergisTek, a healthcare security consulting firm. “As a result, we’re now seeing hacks and threats aimed at healthcare that you might not see in the financial sector or credit card industry.”

In 2015, more than 113 million health records were compromised, according to the Department of Health and Human Services Office of Civil Rights. Hackers breached the personal information of tens of millions of customers of the health insurers Anthem and Premera Blue Cross. In early 2016, hackers infected the networks of a handful of hospitals and broader health systems across the country with ransomware, malicious programs that hold patient records hostage and enable the hackers to demand a ransom to return them. The persistence of cyberattacks on hospital networks now makes healthcare the most frequently attacked industry, beating out the financial and retail sectors, and costing the industry $5–6 billion a year.

“We have all the best data that the bad guys want because we collect so much information about patients,” Finn said. “Their demographic information alone would be good enough to start doing some bad things, but then you add data like credit card numbers, insurance account numbers, and Social Security numbers, and it really is one-stop shopping for them.”

Even more concerning, as foreign governments increasingly turn to cyber-espionage to gain intelligence about the United States, hackers gain new sources of funding. “Sometimes espionage is all about socioeconomic gathering,” said Mac McMillan, the CEO and co-founder of CynergisTek. “There’s nothing more lucrative to a foreign government than gathering that kind of information about the health of our population.”

Labs at Risk

Increasingly, hackers penetrate hospital networks by infecting medical devices with their malware and ransomware, using out-of-date instruments as holes in the system. This tactic adds a new kind of threat beyond the better known use of emails or clickbait to infiltrate servers. “In 2015, we saw an awful lot of cardiology intervention centers and catheterization labs get shut down because of malware,” said Finn. “The year before, we saw the medication cabinets in nursing areas get infected.”

Labs—like cardiology centers, nursing stations, and pharmacies—often have their own record systems, devices, and IT support that operate independently of the broader hospital or healthcare system. In IT, these silos pose particular risks. For example, when information passes between silos, it often presents a weak spot for hackers to access. Moreover, devices run within silos...