MDS Alert

Cybersecurity: Don't Get Lax on IT Security

Aggrieved workers constitute a real threat for organizations.

As if the long-term care industry didn't have enough on its plate already, the Department of Health and Human Services (HHS) Health Sector Cybersecurity Center is warning healthcare organizations to remain alert to cyber threats.

Even if your staff are regularly educated on how to avoid external threats, is your organization prepared to deal with threats that may arise from frustrated staff?

Update: On April 21, the Department of Health and Human Services' Health Sector Cybersecurity Coordination Center (HC3) added a new warning on insider threats to its online resources. The alert offers statistics, advice, and tips on how to identify and address insider threats.

Any person - including employees, vendors, and contractors - with access to your IT and business assets could be a threat to your practice and "could use this information in a way that negatively impacts the organization," explains the HC3 brief.

According to the Ponemon Institute's 2020 Insider Threats Report, 61 percent of internal issues are caused by "negligent insiders," with 25 percent attributed to insider incidents related to credential theft. Most of these incidents aren't intentional and are caused by a "lack of awareness about security policies and a failure to provide security awareness training," the report maintains.

However, "malicious insiders" with a "grievance against the company" are still a concern and should be on your radar, HC3 says. These disgruntled staff account for 14 percent of insider threat incidents and can wreak havoc on your organization, according to the Ponemon Institute report.

Look for Clues Indicating Security Issues

Data security incidents usually don't just pop up. In fact, there are three sets of indicators to look for that can help you identify a potential incident. Here's a brief overview of the trio of indicators, according to HC3 guidance:

1. Behavioral: Unusual or odd behavior from your staff or business partners may warrant an extra eye. Malicious insiders may be prone to personality conflicts with other employees, may engage in office bullying or unprofessional behavior, or may fight with managers and co-workers, HC3 suggests. Other signs to look for include "official records of security violations or crimes" and misusing practice time and money.

2. IT sabotage: Insider threats that aim to take down your systems through sabotage are not always easy to spot. Accessing other employees' computers, disabling monitoring and logging systems, and changing login and password information without permission are all indicators of malicious activity. Nefarious software installation may go unnoticed, so it's critical that IT staff keep on top of software updates and check for new account creations, remote access software, and malware infiltrations.

3. Data theft: With remote work at its height, it's important to watch for unauthorized access to files and data, especially if an employee is trying to access practice servers during non-working hours. Other data theft clues include excessive emailing of corporate or sensitive data to a personal email, attachment-heavy emailing to non-corporate emails, "massive downloading of corporate data," and "excessive use of corporate printers," HC3 warns.

Guard Against Threats With These Tips

As part of the HIPAA Security Rule, covered entities (CEs) must design and implement a security plan. Training employees on cybersecurity concerns, including identifying insider threats is key to the success of your overall compliance.

Why? Staff are often nervous about calling out other employees or telling management about unusual network activity they may have noticed. They may feel like a breach is too minor to even mention - and that's why cultivating compliance is so crucial.

"Train in incident management, top to bottom," advises **Jim Sheldon-Dean**, principal and director of compliance services for Lewis Creek Systems LLC, in Charlotte, Vermont. "Staff need to feel like they are empowered to report their suspicions of information security incidents, the handling of incidents needs to be clearly defined, and top management needs to understand the impacts of incidents and the necessity to prevent them as reasonably practicable."

Resource: Check out more tips and tools on insider threats at www.hhs.gov/sites/default/files/insider-threats-in-healthcare.pdf.