AUDITBOARD

Top 5 Cybersecurity Concerns for Healthcare Auditors

The post-pandemic world has created new and more challenging cybersecurity risks for the healthcare industry. By combining the trends in data breach disclosures with the increases in work from home policies and in the level of stress and fatigue prevalent in healthcare workers, there are five risk concerns that internal auditors must keep on their radar.

The top five cybersecurity risks are:

THE TOP FIVE CYBERSECURITY RISKS	
1	Phising
2	Shadow IT
3	Endpoint Exposure
4	Data Piracy (ransomware)
5	Cloud Computing

1. Phishing

The increase in phishing attacks continues to rise dramatically. The Blackbaud event alone involved dozens of providers and millions of customer records. Over the years, phishing has been responsible for the majority of the cyberattacks on healthcare. **A report from IBM found that 95% of breaches are caused by human error**. Most breaches are caused by an end user clicking on something they shouldn't — such as a phishing scam, which accounts for 90% of security breaches according to the same IBM report. Now that many frontline workers are experiencing higher levels of fatigue, they are more likely to open phishing emails without considering the implications.

2. Shadow IT

Shadow IT refers to Non-IT Departments buying technology like software and hardware without the IT Department's knowledge. The problem also extends to web-enabled devices or Internet-of-Things (IoT) equipment. Adding unsupported software and unpatched devices to the environment can drastically increase the risk of exposure. **Shadow IT exposure adds to the existing risk associated with people using personal devices to connect to your network.** When employees go rogue, your entire network is open to their personal security practices, no matter how good or bad.

3. Endpoint Exposure

With the rise in people working from home, the endpoints connecting to your network have increased exponentially. Similar to the Shadow IT risk, your network can be exposed through the employees endpoints that are outside of the firewall including laptops, mobile devices, printers, and IoT devices like voice assistants, thermostats, and refrigerators that have internet connections.

4. Data Piracy and Ransomware

UCSF Medical school had to pay $1.14M in ransom to hackers who stole their data and hijacked their servers. **The hackers usually gain access by deploying ransomware through phishing emails or manual deployment in a compromised network.** Vulnerability scans, anti-spam, and anti-phishing, and frequent offsite backup routines help prevent the attacks and mitigate the risk if the network needs to be restored.

5. Cloud Computing

Cloud computing has seen huge usage increases over the past 5 years. **Hackers are primarily using remote exploitation of cloud applications to gain access to the cloud environment.** They are also using security flaws introduced by end user configurations of the applications that connect to the cloud. The most common cause of these two weaknesses is employees setting up cloud applications on their own without the help of cloud security professionals.

Conclusion

Internal audit has a critical role to play in advising management on the risks that can prevent the organization from achieving its strategic objectives. **In healthcare, cybersecurity is consistently one of the most critical and costly risk exposures.** As you continuously update your audit plan, it is more important than ever to evaluate the cyber risk landscape while considering the impact of people working from home and working under extreme stress.
