Codify
BY AAPC

Health Information Compliance Alert

Cybersecurity: Alert Leadership to the Risks of Cyberattack

Communication is key to circumventing IT issues.

Whether you're the chief information security officer (CISO) or in charge of securing your organization's network and devices, the time will come when you need to inform executive leadership of emerging cyber threats.

Learn how to effectively communicate cyber threats to C-suite executives.

Are Executive Leadership Aware of Cybersecurity Risks?

According to a PwC survey released in January 2022, 49 percent of global CEOs consider cybersecurity risks to be the leading business risks. Healthcare executives are very aware of cybersecurity risks and the damage a data breach, ransomware attack, or phishing scam can cause on a healthcare organization.

At the same time, the U.S. Securities and Exchange Commission (SEC) March 2022 rule proposal would hold executive leaders and board of directors responsible for an organization's cybersecurity controls, if finalized. Elevating cybersecurity risks to the boardroom helps make the constantly emerging threats a top priority for the executive leadership.

In addition to the SEC's proposal, C-suite leadership looks at cybersecurity risks as major problems to ensure proper care. "Successful ransomware attacks and consequential business disruption have also contributed to the interest of executive leaders in implementing appropriate cybersecurity controls to minimize adverse impact on healthcare operations," says **Funso Richard, CISA, CISM, CDPSE, CCSFP, CHQP**, information security officer at Ensemble Health Partners in Cincinnati, Ohio.

While the executives are aware of the dangers of cyber threats, effectively communicating the gravity of the risks can be tricky even for seasoned CISOs.

Know What Information Demands Attention

With new cyber threats emerging constantly, you need to provide executive leadership with reliable communication regarding possible hazards. By creating a risk assessment report, you can effectively communicate a potential data breach threat if appropriate data loss controls aren't implemented simply by using data from other compromised healthcare organizations.

Part of that communication is understanding your firm's risk exposure and knowing what to relay to the C-suite. When there is an ongoing threat, having all the answers can be challenging. By performing a reasonable assessment, the CISO can better understand what threat the practice is facing and which containment plan to enact.

As a threat arises, you should focus on the following in your threat status report:

- Type of threat and scope of impact gathered from the reasonable assessment
- Steps implemented to contain the cyber threat
- Action(s) to remediate the impact
- Additional controls implemented to help prevent future attacks

"Threats become successful when risks have not been reasonably identified and mitigated. The goal is to effectively communicate risks to reduce cyber threats," Richard says.

Takeaway: Prepare a concise threat status report that relays what steps you're taking to tackle the threat.

Remember, Time Is Valuable

When time is a factor, such as when securing a cyber threat before it can attack your network, details aren't what executive leaders are seeking. They don't have time to consume a detailed cyberthreat intelligence report. If you're a CISO, your report to the C-suite executives should focus on the impact that unpatched systems could have on your organization's bottom line rather than the specific number of unpatched systems on your network. "When presenting a cybersecurity risk report, CISOs should prioritize the information that directly affects the business," Richard says.

However, if you work in a small practice where you wear multiple hats, including IT and cybersecurity, talking to executive leaders may seem intimidating. In that case, your best bet is to be direct with leadership. "If you want their attention, you must focus on the results. Don't ramble. When you have to discuss the problem, you need to talk about its effects on outcomes," said **Rhonda Buckholtz, CPC, CDEO, CPMA, CRC, CENTC, CGSC, COBGC, COPC, CPEDC**, Approved Instructor during her session, "Elevate Your Communication Style: Talking to the C-Suite," at AAPC's 2021 ELEVATE Conference.

For example, a successful phishing email attack can lead to data breaches and other disruptions to your healthcare organization. "When presenting a report on a phishing email attack, the CISO should include the number of phishing emails successfully stopped, those that made it through, and the number of employees who fell for them," Richard says. He continues to add that remedial education and implementing controls to help prevent future failure are also critical to include in your report.

Takeaway: Create an efficient report with information that directly affects the business operations, as well as steps taken to retrain employees and help prevent repeat attacks.