SECURITY NEWB
By Kacy Zurkus ★ Advisor

OPINION

Bringing cyber awaren

Different approaches to char

CSO | Oct 12, 2016 5:11 AM PT

Yesterday's post offered some expert advice in developing a corporate culture around cybersecurity. While it would be great to hear more water cooler conversations that include Dark Net or Mr. Robot, change is a process. But, don't give up hope that your efforts are ineffective.

Rather, continue to look for ways to change culture not only at the employee level but also at the executive and board level. Often times, executives feel that they are immune to the tricks of social engineering, but we've seen otherwise with impersonation emails.

Tip number one is to remember that everyone is a potential target and no one is beyond reproach. Leave your ego at the door.

Then what? Well, here are some more tips from industry experts on how to approach insider threats and the board as well as expand your awareness of threat vectors.

Kon Leong, President, CEO and Co-founder, ZL Technologies said:

The most immediate security threat often comes from within. This isn't always caused by malicious behavior; it also results from misinformed employee data practices. Luckily, advancements in technology have enabled data control through capabilities such as employee access privileges, ensuring data stays in the hands of the people who need it. Optimizing these capabilities requires a command of data only possible through comprehensive information governance.

However, security technology is not something you simply plug in and forget about: End users must be brought into the equation. They're the ones who know best the content of the data they create, so consulting with them to set proactive access privileges and retention policies is essential to risk mitigation.

Making cybersecurity a collaborative process will promote a risk-oriented culture within the organization. Whether training end users or engaging in board discussions, a focus on collaboration across all departments will help to improve your corporate culture.

Guy Caspi, CEO, Deep Instinct offered this advice:

Businesses need to change their approach to cyber-attacks. Instead of waiting for an almost imminent attack, they need to think like their attackers.

Conduct vulnerability assessment and penetration testing. It's all about testing the network and the applications from the technical side. Conduct a vulnerability assessment to discover the flaws in your system. Once you have identified the flaws that can be exploited, conduct penetration testing to carry out attack-simulated scenarios, gain an in-depth understanding of its degree of severity and how it can be remediated to avoid a real-life exploitation.

Invest in cyber education: Raise awareness about phishing emails and set a procedure on how to handle them. Additionally, test your staff's degree of diligence and awareness about social engineering, especially those with access to sensitive data.

Involve the Board of Directors: As trustees of the organization's value and growth, it's critical for boards of director to start weighing in on cybersecurity activities similarly to their oversight on the financial ones. When addressing the issue, use language focusing on organizational growth, operations and value. This enables the directors to evaluate the overall cybersecurity risks and management activities, as well as decide upon an agreed level of risk, especially in the event of post-breach liabilities deriving from regulators, the media, and even potential plaintiffs.

Evan Blair, Co-founder and Chief Operation Officer, ZeroFOX said:

Social media represents the largest modern threat vector: it's got more connectivity (billions of people), it's more trusted (everyone is your friend) and it's less visibility (simply by its nature) than any other communication or business platform. Security teams need to join their sales, marketing and customer success groups in the digital era, implement risk monitoring and remediation technology around social media to secure their organization's future.

Security team's responsibilities:

- Work with marketing to gain access to social accounts
- Continuously monitor corporate social media accounts for cyber threats
- Blacklist/block malicious URLs and IPs found on social media
- Establish workflow for dealing with social media cyber crime targeting the organization
- Takedown malicious posts and profiles
- Test employees on susceptibility to social media cyber attacks
- Train employees on safe usage, best practices, and what to do in the event of an attack
- Work with marketing to keep a close eye on social media initiatives and campaigns

This article is published as part of the IDG Contributor Network. Want to Join?

Kacy Zurkus

★ **Advisor** | IDG CONTRIBUTOR NETWORK

Kacy Zurkus is a contributing writer for CSO covering a variety of security and risk topics.

Insider: These ransomware situations can result in colossal outcomes

View Comments

You Might Like