Increase in Cybercrime

Demands Fresh Attention to Employee Onboarding and Training

By Terri Howard, Contributing Writer

Cybersecurity training should be treated as an ongoing process and include employees across an enterprise's footprint.

Until the massive U.S. Target store credit and debit card data breach in 2013, the lasting impact of cybercrimes was a relatively unknown experience to most consumers, and it wasn't on the top list of HR onboarding topics either. Flash-forward to today, and cyberattacks, hacking, data breaches and identity theft are household terms, and the need to educate employees about how their actions impact company cybersecurity is greater than ever.

The likelihood of a damaging cyberattack has grown with the role of technology in the business landscape. For every high demand UX developer and software engineer, there is someone else using the same skillsets to hack corporate systems. The question for companies is no longer "Will I be the target of a cyberattack?" but rather "When?" Yahoo learned this the hard way, as did health insurer Anthem Inc., Sony Entertainment, the Democratic National Convention, and even the Internal Revenue Service, to name a few.

Yet, as common as news headlines have become, a recent study conducted by International Data Corp (IDC) found most U.S. companies are underprepared to deal with cybersecurity threats. Even though there are lots of good best practices, they're only being conducted by a small number of leading-edge firms.

While IT and cybersecurity professionals are experts at protecting networks and devices, and integrating security measures to anticipate a breach that cannot serve as an organization's be-all, end-all response. Employee education and training can help minimize cyber vulnerabilities and prepare employees for the event of a breach, in turn helping to protect the organization and its customers.

What Makes a Company Vulnerable?

Employees often are unaware of the potential consequences of their actions when working on a computer, laptop or mobile device and how those actions can open a company up to attacks. According to the United

States Computer Emergency Readiness Team, it's important to remind employees of the critical role they play in protecting the company from cyber threats.

The onboarding process starts with making the right hires. Background checks on potential candidates should be standard operating procedure. As new employees join the workforce, organizations also need to take extra precautions to be sure they have an effective training plan in place.

As part of the onboarding process, new employees should be warned to:

- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known. Be particularly wary of compressed or ZIP file attachments.
- Avoid clicking directly on website links in emails. Instead, users should type the link directly in the browser's search bar or attempt to verify web addresses independently (e.g., contact the organization's help desk or search the Internet for the main website of the organization or topic mentioned in the email).
- Log off or use a screen saver when not in front of computer.
- Report any suspicious emails to the help desk or security office immediately.
- Avoid unsecure Wi-Fi hotspots. Offering employees the perk to work from home or off-site at the local coffee shop sounds great, but from an IT standpoint, it could be a nightmare. Any time an employee connects to public Wi-Fi, the data on a company's server is open for hacking. Airport and hotel Wi-Fi is another concern for employees who travel frequently.
- Be smart about peer-to-peer file sharing. Sharing files via flash drive is akin to college students sharing a drinking cup. Instead of spreading germs, the drives potentially spread viruses.
- Follow company guidelines and restrictions for social networking sites like LinkedIn, Twitter, Facebook and Instagram.
- Consider putting a social media policy in place if you do not already have one.
- Avoid downloading software or apps from unknown sources.
- Maintain good password integrity.
- Avoid sites at risk for malvertising.
- Be smart about laptops or mobile devices that float between systems and could therefore pick up viruses or compromise the system.

After reviewing technology protocols with new hires, don't be afraid to test the policy. Send a mock-questionable link to employees to see if they click on it, and implement consequences when an employee leaves the company open for a cyberattack. Cybersecurity training is not a one-time event or something that only applies to the IT department. It should be treated as an ongoing process and include employees across the company's footprint.

Specialize Your Training

Beyond new hire training, most organizations will have an identified disaster preparedness team. Go a step further to bring that team up to speed on Cybercrimes 101 as well. While smart onboarding policies help prevent breaches, this type of training prepares your team for a breach response. What are common types of attacks? How does the scope of damage change based on the hackers' motivations? What unique challenges are present when large data breaches occur? And how would the company be prepared to assist in victims' recovery – emotionally and in terms of compromised identity or security?

During initial discussions, it often helps to rank potential threats in a matrix, from Least Likely-Least Damaging to Most Likely-Most Damaging, to account for a particular company's highest risk areas. By doing so, your team can prepare for cybercrimes in the same way it might prepare for workplace violence incidents or natural disasters.

Dealing with a breach of customer or employee information will involve a variety of departments: executive leadership, communications, customer relations, HR, the organization's employee assistance program (EAP) and possible outside support to funnel inquiries and concerns.

When outlining an organization's cybercrimes threat matrix, highlight particular trouble areas and work with communications or HR to share best practice protections with the entire workforce. A basic internal education effort likely will look at aspects including:

Types of Attacks

Review the nature, probability and dangers of common attack methods like hacks, breaches, and phishing via email, texts or social media. Also review common entry points or data-rich targets within a company. Any system with data that can be monetized – health care records, bank information, credit card numbers, emails – can pose a risk and should be part of the response planning process. In the Target breach, attackers gained access not only to card numbers, but also card expiration dates, CVV codes and cardholders' names.

Types of Motivation

Provide general background on the different categories of cyberattacks and how the scope, style and motivations of each play an important factor in developing the most appropriate response plan.

- Cyber criminals are motivated by money and are typically responsible for hacks like retail data breaches and phishing attacks. There is high risk to individual customers in terms of compromised personal or financial data and identity theft. The 2015 breach of Anthem Health Insurance is a good example of this.
- Nation-states engage in cybercrimes to gain intelligence or sow disruption. The danger here is centered on corporate or industry infrastructure – everything from Wall Street to transportation to the electric grid – or on massive data collection, though the ramifications often spill over to individual consumers through city-wide loss of services.
- Hacktivists are most likely after small-scale disruption, embarrassment or justice seeking, rather than personal financial information. Think of the hack on site Ashley Madison or the work of groups like WikiLeaks or Anonymous. These types of attacks lead to deep emotional pain and privacy violations.

Take the education a step further by displaying tip sheets and posters around office common areas or by participating in ongoing cyber safety events like National Cyber Security Awareness Month or Safer Internet Day. Companies that do not onboard new hires or continually educate employees on ways to prevent cyberattacks and properly respond if they occur are the most vulnerable. Keeping the issue top of mind for your team helps mitigate risk and build resiliency. S

About the Author

Terri Howard, Senior Director at FEI Behavioral Health, is responsible for working with corporate clients to ensure companies are prepared for, can respond to and recover from a crisis incident. She also coordinates the people support and psychological first aid services for those impacted by a crisis incident and is experienced in developing drills and exercises aimed at testing current crisis management plans and procedures.