Improving the Effectiveness of Cybersecurity Training

While cybersecurity training programs aim to teach employees to spot potential threats, avoid common errors and report suspicious activity, many fail to meet these goals. Traditional cybersecurity training programs have often focused heavily on compliance rather than practical behavior change or relied on generic training materials that are easily forgotten. When cybersecurity awareness is poor among workforces, companies may be at greater risk of cyberattacks. Specifically, ineffective training may fail to reduce human error rates, such as susceptibility to credential theft, social engineering tactics and common mistakes that expose information or systems to risk, leaving organizations vulnerable. Ultimately, when training is ineffective, both the likelihood and impact of cyber incidents may increase. To improve the effectiveness of their cybersecurity training programs, organizations should consider the following tips:

- **Shift to continuous reinforcement-based learning.** Organizations should deliver training in small, focused segments that target a single behavioral objective, rather than broader annual compliance exercises. Known as microlearning, this approach can reduce cognitive overload and may solidify memory pathways. It may also be easier for employees to incorporate microlearning into their daily routines, increasing engagement. For example, rather than delivering a single long session on phishing awareness, organizations could provide multiple shorter sessions on related topics, such as identifying suspicious links, recognizing email spoofing and practicing password hygiene.
- **Personalize content by role.** Organizations should adapt training materials to the specific responsibilities, risks and experience levels of different employee groups. When training reflects real workplace situations, employees may find it easier to understand how it applies to their daily tasks, making content more meaningful. For example, finance team training could focus on phishing scams targeting invoices, while IT teams might explore detecting insider threats or responding to system anomalies. Overall, training materials should directly address the intended audience, incorporate realistic scenarios and align with each department's objectives.
- **Use engaging and active methods.** Organizations should consider incorporating game-like elements to make training activities more fun and engaging, a practice known as gamification. This approach uses interactive elements (e.g., quizzes, challenges, badges, leaderboards) to promote active participation and keep employees motivated. Organizations should also arrange hands-on exercises that allow employees to practice threat responses in real time. For example, employees could participate in short phishing-spotting competitions, complete quick challenges to verify sender identities, or review anonymized examples of past organizational security events to understand how certain actions contributed to breaches.

Contact us today for additional cybersecurity guidance.

Fostering a Cybersecurity Culture

Employees are widely considered top targets during cyberattacks, making them an organization's first line of defense. In fact, a joint study by Stanford University and cloud email security company Tessian found that the vast majority (88%) of data breaches stem from employee mistakes. For this reason, it's vital for organizations to make cybersecurity a priority for the entire workforce and an integral part of company culture. Creating a solid cybersecurity culture can offer various benefits, including strengthened protection against digital threats, increased customer loyalty and improved brand reputation. The following best practices can help organizations establish an effective cybersecurity culture:

- **Involve senior leadership.** Employees need to see cybersecurity values upheld by management if they're going to uphold such a culture. With this in mind, organizations should encourage senior executives to take digital threats seriously and lead by example.
- **Inspire ownership.** Organizations should clearly communicate the risks of poor cybersecurity measures to their employees and outline the steps they need to take to minimize digital threats.
- **Bring back the basics.** When promoting good cyber hygiene, organizations shouldn't neglect the basic principles within workplace policies and procedures, such as strong password requirements, multifactor authentication protocols, network access restrictions and safe download standards.

- **Maintain secure communications.** Organizations should ensure employees understand how to report suspicious emails and verify the authenticity of all work-related communications.
- **Celebrate success.** Making cybersecurity part of performance reviews and reward programs can help organizations formally recognize and motivate employees who demonstrate a commitment to defending against digital threats.

Encouraging employees to value and take responsibility for cybersecurity is a proactive way for organizations to reduce the risk of cyberattacks. By fostering a strong cybersecurity culture, organizations can minimize digital threats and limit potential losses in the event of cyber incidents.

Debunking Common Cybersecurity Myths

Cybersecurity has become more important as organizations expand their reliance on technology and other digital services in their operations. After all, cyberattacks can carry serious consequences, including damaged data and systems, prolonged business disruptions, diminished customer loyalty, lost revenue and costly regulatory penalties.

Even so, some common cybersecurity myths can undermine the perceived severity of potential threats and diminish the value of effective mitigation strategies. If organizations assume these myths to be true, they could leave themselves increasingly vulnerable to cyberattacks and related losses.

Here is the reality behind three common cybersecurity myths:

Myth #1: Cybersecurity is the IT department's job.

Even when organizations make the wise decision to invest in cybersecurity, they may still place all related responsibilities on the IT department. Although these professionals play a role in upholding adequate cybersecurity measures, they can't act alone. The most effective cybersecurity models involve companywide participation, which requires support from corporate executives and routine training for all employees.

Myth #2: Cybersecurity measures are only necessary for large corporations.

Large organizations are susceptible to cyberattacks, but this doesn't mean small businesses are immune to such incidents. On the contrary, some cybercriminals consider small organizations more attractive targets than their larger counterparts because these businesses are more likely to have weaker cybersecurity measures in place.

Myth #3: Cyberthreats are always external.

When most employers and employees picture a cybercriminal, they likely visualize an external threat actor. Nevertheless, cyberattacks can also arise from insider threats (e.g., an employee, vendor or third-party collaborator). Due to their unique access privileges, insider threats can compromise organizations' most valuable assets and leave them more susceptible to a range of cyber incidents (also called insider events).

Contact us today for further risk management resources.

This Cyber Risks & Liabilities newsletter is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.