Courtesy of
Connor & Gallagher OneSource

Improving the Effectiveness of Cybersecurity Training

Workforce cybersecurity training is a critical part of a company's security risk management program. Cybercriminals don't just target systems, devices and networks; they frequently target employees, who may use weak or reused passwords, fall for phishing scams, or click on dangerous links or attachments. In fact, 68% of cyber breaches involve a nonmalicious human element, according to a recent report by telecommunications firm Verizon.

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. Since employees are a company's first line of defense against cyberthreats, it's vital that organizations ensure their cybersecurity training is effective.

This article discusses why many traditional training models fail, the implications of ineffective training and how organizations can improve their cybersecurity training programs.

The Training Retention Problem

Training programs that are dense in information can be undermined by the "forgetting curve," originally coined by German psychologist Hermann Ebbinghaus in the 1880s. Research by Ebbinghaus found that roughly 50% of new information is forgotten within one hour, 70% within 24 hours, and up to 90% within one week. Modern research continues to validate the idea of memory decline. Training research also indicates that employees may forget a significant portion of training content within a short period if they do not apply or revisit it soon after learning.

Traditional training models may also fail to achieve their objectives due to the following reasons:

- **Passive delivery**—Corporate training programs often rely on passive consumption of information, such as reading long manuals or watching lengthy videos. When cybersecurity content is delivered passively, it can feel like a chore rather than valuable education, particularly when employees are busy. As a result, workers may rush through the material, treating it as a checklist exercise rather than something to give their full attention.
- **One-size-fits-all approach**—Cybersecurity training is often generic, divorced from real-world application, and fails to address the specific learning needs of participants. When training lacks relevant context, employees may struggle to see its purpose, reducing engagement.
- **Overemphasis on compliance**—Many training programs are designed to meet regulatory requirements or pass security audits. As such, they can become annual checkbox exercises that focus on completion rather than comprehension. When compliance is the goal, training may fail to build genuine understanding or translate into secure day-to-day behavior.

Implications of Ineffective Training

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. Research consistently finds that phishing and credential theft are among the most common initial access vectors in cyberattacks. As such, a single employee mistake (e.g., clicking a malicious link) can unintentionally trigger a major cyber breach that exposes an organization to significant losses. Such incidents can lead to operational disruptions, reputational damage and regulatory or legal exposure. Ultimately, when training is ineffective, both the likelihood and impact of cyber incidents may increase.

Best Practices to Improve Training Effectiveness

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 focus on single behavioral objectives, instead of broader annual compliance exercises. Known as microlearning, this "little and often" 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 one long session on phishing awareness, organizations could provide multiple shorter sessions on related topics such as identifying suspicious links, recognizing email spoofing and practicing good 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, training for finance teams could focus on phishing scams that target 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 fun and engaging, 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.

Reinforcing Learning Through Culture

For training to be fully effective, organizations must reinforce it with a culture of accountability and leadership support. Rather than a one-off training event, cybersecurity should become an integral part of company culture and be talked about regularly. Leaders should reinforce the importance of cybersecurity training, embed cybersecurity into strategic decision-making and consistently model secure behaviors. Organizations could also identify "security champions": influential employees who can advocate for security awareness among their peers and share tips and lessons learned during team meetings or informal conversations.

Making Reporting Easy and Nonpunitive

A strong security culture also depends on making reporting easy and nonpunitive. Organizations should foster psychological safety by encouraging employees to express ideas and concerns openly. Minor errors should be seen as learning opportunities rather than grounds for punishment, and there should be clear, accessible channels for reporting suspicious activity. Encouraging reporting without fear of blame can promote early threat detection and strengthen overall security awareness.

Measuring and Continuous Improvement

Since cyberthreats continually evolve, organizations should regularly review the effectiveness of their cybersecurity programs to ensure they are meeting company objectives and staying aligned with current risks. Key metrics to track include phishing success

rates, training completion rates, incident response times and simulated threat exercise results. It may also be prudent to survey employees to gauge how they are finding the training and identify any gaps in knowledge.

Conclusion

Cyberattacks remain a persistent threat to organizations of all sizes, and human error is a leading cause of many breaches. Organizations can reduce their exposure to cyberthreats by strengthening their cybersecurity programs and fostering a culture of security awareness and accountability.

Contact us today for additional cybersecurity guidance.