Texas Council Risk Management Fund

Importance of Consistent User Cyber Training

Cyber security has been going through a transformation in recent years. As training for employees was typically centered around new technical advances, software, and process development, the proliferation of cyber threats like phishing and social engineering attacks has forced organizations to shift towards training employees to help combat cyber-attacks.

Most cyber threats exclusively target individuals. Users represent a potential point of failure in defenses. With consistent cyber training, users can become a line of defense and act as a reliable cyber security measure.

The challenge is designing a training program that keep users interested while giving them a sense of the importance of cyber security. This coaching must also be built to consider varying levels of technical skill and different roles.

There are methods to keeping users engaged while boosting information retention, but before you start a training program, it's important to know what you're working with so you can lay out the most efficient plan for your organization. It's a good idea to have either a formal test or phishing simulation to get a good baseline of your employees' skill level. The frequency of the cyber security training should also be based on the data you collect from the prior training. Are users clicking on phishing simulation emails? Does the staff seem to struggle with certain concepts? No matter the size of your organization, cyber security awareness programs should be reviewed and updated at the very least every quarter. Reviews should focus on a couple of objectives:

- Identify the **areas** where employee behavior has the most significant impact on overall cyber-risk levels. Prioritize training topics for the areas.
- Identify **employees**, based on their roles, whose behavior most significantly affects overall enterprise risk levels – for example, those with elevated administrative privileges or with access to protected data. Prioritize their training and consider engaging them in more extensive and frequent training than regular users.

Consider sharing stories of real-world attacks that audiences can often find engaging. While discussing actual events, trainees can learn from these internal or external incidents.

Because people learn in different ways, cybersecurity awareness training requires a varied approach. The more mechanisms an organization uses to train, the more likely the knowledge reaches members of the target audience.

Consider the following training formats:

- On-demand video training.
- Interactive training modules, available from third-party service providers such as KnowBe4, and Proofpoint.
- Short discussions in team meetings about cyber hygiene and security awareness.
- Informational posters in high-traffic areas of the office, such as kitchens and break rooms.
- Educational lunch-and-learn sessions.

Cybersecurity awareness training is an ongoing operation. It should start with the onboarding process and continue throughout the user's tenure at the organization. It helps to view cybersecurity awareness training as a muscle memory exercise. To get the full benefit, employees must be regularly engaged with security simulations, and tests, through a variety of different exercises.

The TCRMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments and Incident Response Plan Tabletop Testing visits for members. To get on the schedule email Lee Cain, Cyber Risk Services Advisor lee.cain@sedgwick.com or give him a call at (512) 619-1437.