The Main Problems and Setbacks of Cyber Security Training

Devolutions

AS A BUSINESS, YOU'RE ALWAYS AT RISK OF A CYBER SECURITY BREACH OR ATTACK

As a business, you're always at risk of a cyber security breach or attack. Your employees are a big part of assessing various levels of risk, so you need to make sure they're properly equipped. A lot of digital attacks look to exploit the human element via phishing attempts. Malicious attackers will try to trick users into giving them access to a digital database or resource before trying to fully hack into the system. Here, we'll explore why humans are so vulnerable to cyber attacks, and why employees must therefore be highly trained in cyber awareness to avoid falling victim to malicious schemes.

The Importance of Security Awareness Training

Although a lot of business processes are being taken over by automation and technology, organizations still need humans to take care of most business and customer interactions. The simple and repetitive tasks are automated, but the key decisions still require people. These people comprise the human factor commonly targeted by hackers. To defend against a wide variety of cyber attacks, security awareness training is key.

According to Luke Morris, a tech writer at Brit Student and Write My X, "because the cyber environment is constantly changing, and there are so many different vulnerabilities, security training cannot be a one-size-fits-all approach. It has to be repeated frequently, updated all the time, and tested constantly."

Best Practices

Cyber security best practices include: compliance with all local and federal laws and regulations; coordination between all organizational levels; an established baseline for all assessments; and the creation of a clear communication system. In terms of the actual training, it has to be somewhat engaging and intriguing, as well as constantly reviewed and enforced. This is the only way to make sure there's an environment and culture at work that supports continuous learning and vigilance.

These best practices are a great starting point when developing your organization's security awareness education program. Of course, each organization's security situation is different and will require tailored solutions, but the overall goal and objectives will be similar in kind.

Goals and Objectives

The main goal of developing a security awareness program for your staff is to render your company more secure. If your business has sensitive data, then you need to secure that information in order for your company to be successful as you move forward. Whatever goals you establish, they should all be in line with the overall purpose of your security program. At the end of the day, you would ideally like to have 100 percent awareness of all electronic and software-based threats.

Your goals should begin simply — from creation to delivery to evaluation. With time, your quarterly and annual goals will be increasingly tied to the possibility or actuality of incidents in the organization. Cyber attackers are constantly on the lookout for new weaknesses and new ways to exploit an organization, so you must have a proactive and flexible program.

How to Start

The first issue to assess is your business' security training requirements by making an individual assessment of each employee. You should then think about how to deliver such security training requirements — whether in person, online, or by video. As per Kelsey Daniels, a security analyst at Australia2Write and Next Coursework, "depending on what you choose, you'll have to then create the necessary content, which will be delivered by the security professional in your business. The training material can include posters, email testing software for phishing attacks, on-site presentations, and more."

At this point, it's important to set the expectations for all, including the timing, delivery, requirements, method, and expected results. Be sure to offer lots of different sessions so every employee in the organization can attend. Deliver the training in accordance with your plan and be sure to gather feedback from the employees on the training itself to see what could be improved for the next time. After the training is over, run assessments with all employees to figure out how effective your training was and how much was retained.