10 ways to raise your users' cybersecurity IQ

By Alison DeNisco Rayome

single point of contact

TechRepublic

INTRODUCTION

Employees are a company's greatest asset, but also its greatest security risk.

"If we look at security breaches over the last five to seven years, it's pretty clear that people, whether it's through accidental or intentional introduction of malware, represent the single most important point of failure in terms of security vulnerabilities," said Eddie Schwartz, chair of ISACA's Cyber Security Advisory Council.

In the past, companies could train employees once a year on best practices for security, said Wesley Simpson, COO of (ISC)2. "Most organizations roll out an annual training and think it's one and done," Simpson said. "That's not enough."

Instead, he said organizations must do people patching: Similar to updating hardware or operating systems, you need to consistently update employees on the latest security vulnerabilities and teach them how to recognize and avoid them.

When a user makes a mistake and clicks on an email that causes an infection, we often think that was the cause. But that's not actually the case—the organization was already under attack when the attacker sent the email, before it was opened.

"Your people are your assets, and you need to invest in them continually," Simpson said. "If you don't get your people patched continually, you're always going to have vulnerabilities." Even in a company with hundreds of employees, it's worth training them as opposed to taking on the risk of a breach.

However, it's important to empathize with your employees as well, said Forrester analyst Jeff Pollard. "People represent a large potential attack surface for every organization. The reason I don't like to think of people as a security vulnerability is that it encourages a blame-the-victim mentality. Security teams exist to protect information, people, and the business."

When a user makes a mistake and clicks on an email that causes an infection, we often think that was the cause, Pollard said. But that's not actually the case—the organization was already under attack when the attacker sent the email, before it was opened. It also means every other security control in the path of that attack failed, he added. Here are 10 tips for helping all employees understand cyber risks and best practices.

1. PERFORM "LIVE FIRE" TRAINING EXERCISES

The best training today is "live fire" training, in which the users undergo a simulated attack specific to their job, Schwartz said.

"Maybe they become a victim of an attack that's actually orchestrated by a security department or an outside vendor, and then they're asked to understand the lessons they've learned from that attack, and the implications on the business, on their personal lives and how they could have prevented it," he said. "And then they're asked to share that experience with their peer group."

ISC(2) performs regular phishing tests, in which the IT team sends out a fake phishing email to all employees across the organization and gauges how many people click on it, Simpson said. Then, they can break that data down by departments and types of messages to tailor training to problem areas. It also allows the company to show progression.

2. GET BUY-IN FROM THE TOP

The CISO needs to make the rest of the C-suite aware of the ramifications of a potential breach, Simpson said. "Typically, to have a good cyber plan, you have to have line items in the budget for people, hardware, or software, year over year. That means getting the CFO, CIO, and CEO on board."

3. START CYBER AWARENESS DURING THE ONBOARDING PROCESS

"The first time employees come through the door, start building the mindset as all new hires go through security training from day one," Simpson said. "That way they hear from the time they start that cybersecurity is important and that they are going to get continuous training."

4. CONDUCT EVALUATIONS

Don't be afraid to perform evaluations of both employees and systems to find out how vulnerable your organization is to attack, Simpson said. "Until you do that, you won't know how bad or good your security posture may be."

5. COMMUNICATE

Create a plan for how best to communicate cybersecurity information to all employees, Simpson said, to get all departments on board with training and learning best practices. "It will help break down siloes—it creates alignment, and people working on it together," Simpson said.

6. CREATE A FORMAL PLAN

IT teams should develop a formal, documented plan for cybersecurity training that is reviewed and updated often with the latest information on attack vectors and other risks, Simpson said.

7. APPOINT CYBERSECURITY CULTURE ADVOCATES

Tech leaders should appoint a cybersecurity culture advocate in every department at their organization, Simpson said. These advocates can act as an extension of the CISO and keep employees trained and motivated. "That's something that's often overlooked—use the resources you already have in the company beyond the IT team."

8. OFFER CONTINUOUS TRAINING

Cybersecurity training should continue throughout the year, at all levels of the organization, specific to each employee's job, Schwartz said. "If you're an end user, there has to be training associated with the types of attacks you might receive—for example, attacks on your email or attacks that are oriented to the type of job you hold," Schwartz said. "If you're in IT, the attacks may be more technical in nature in terms of what you might be seeing.

"It really is a case of understanding how the threat landscape continues to evolve relative to these attacks and keeping technical security training current," Schwartz said.

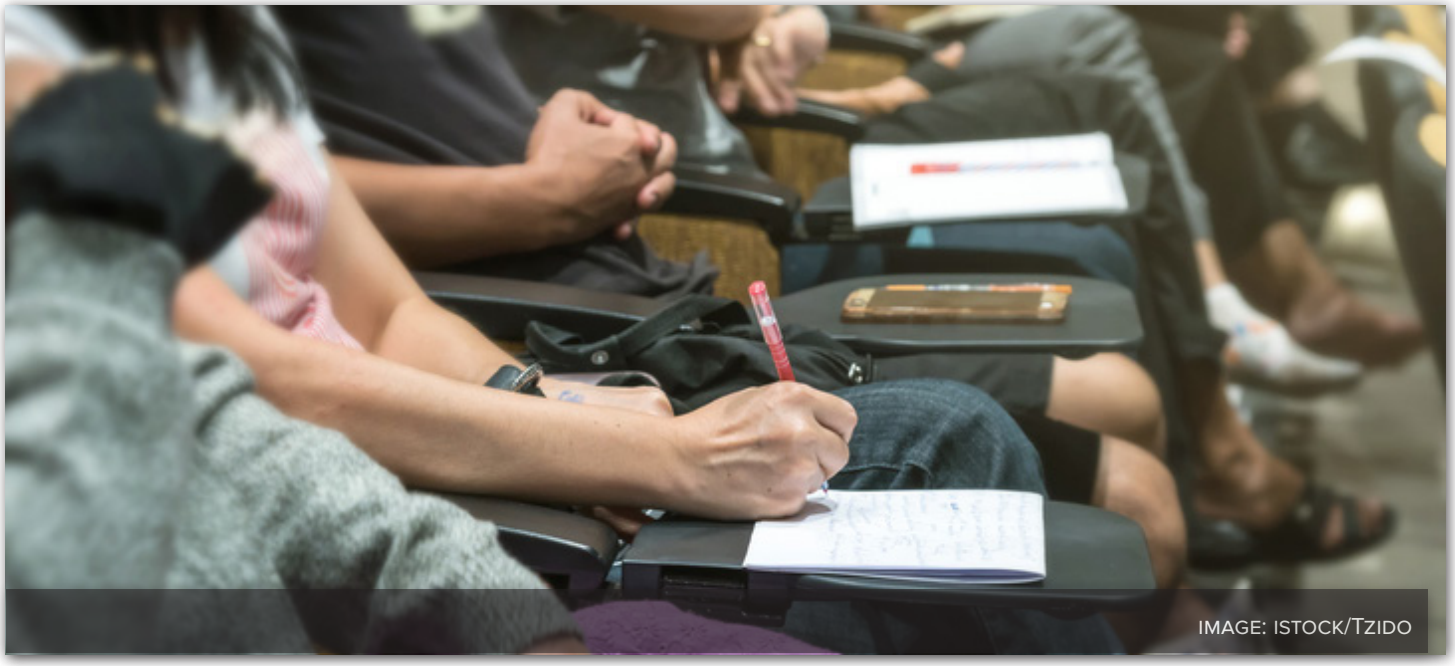

IMAGE: ISTOCK/TZIDO

9. STRESS THE IMPORTANCE OF SECURITY AT WORK AND AT HOME

Tech leaders should help employees understand the importance of cyber hygiene not just in the workplace, but also at home, Pollard said. "Teach users about privacy, security, and how the lessons learned at work can apply at home and in their personal lives to give them a 'what's in it for me' they can apply all the time, not just at work."

10. REWARD EMPLOYEES

Reward users who find malicious emails and share stories about how users helped thwart security issues, Pollard said. IT leaders should also empathize with employees who make mistakes, Pollard said: Many employees send or receive hundreds of emails per day, so asking them to avoid one of those can be difficult.

While these training tips can help, education is not a perfect solution, Schwartz said. "Even in the most advanced and most current education scenarios, there still are a percentage of attacks that will get through, and even in the most enlightening and useful educational programs, there still is anywhere from a 4-6 percent success rate, even after all of the training is done," he said. "So training is just one aspect of defending the environment from advanced attacks."

Contact us

www.singlepointoc.com

Single Point of Contact offers IT security consulting services tailored to your business needs. While we understand there are plenty of layers in security, we will also work with you to ensure you completely understand the advantages of the product or service you are considering for your firm. To learn more about how our services can benefit your organization, don't hesitate to contact us any time.

single point of contact