CSO FROM IDG

SPONSORED CONTENT

skillsoft

metar

PRESENTS

Raising the Bar on Security Awareness

New IDG survey underscores need to foster a data protection culture

Security breaches can impact anyone in the organization, from a low-level employee clicking on an emailed phishing link to the highest executives who must grapple with reputation management and brand damage. Most companies provide some type of security awareness training to counter the threat, but not enough to truly foster a culture of security and keep up with a constantly changing threat environment.

A recent IDG Research survey of more than 100 IT decision-makers found that almost all have experienced security breaches—on average 3.1 types of breach per organization. The respondents represent companies with more than 500 employees in various industries, and just 6% expressed certainty that their organization had never experienced a breach.

More than ever, organizations need to foster a data protection culture to manage risks. This requires security awareness training that is continuous and that evolves along with changing threats.

"In my experience, security training programs typically fall short because there are not a lot of places that let you run scenarios where you hack and defend in a lifelike manner with real consequences, where you switch between hacker and defender, so you understand both sides of the security equation," says Mike Hendrickson, Vice President of Technology and Developer Products at Skillsoft.

The threat is all around us

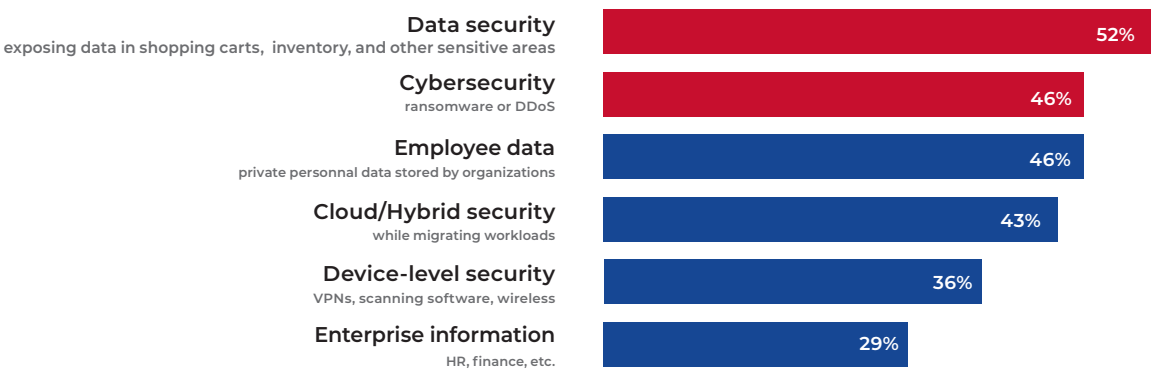
The IDG survey of IT decision-makers found that the leading types of breaches experienced were data security (52%), followed by cybersecurity (such as ransomware) and exposure of private personnel data, both at 46% (see Figure 1).

Companies with more than 2,500 employees were significantly more impacted by cybersecurity breaches (56%, compared to 37% of smaller companies). When it comes to employee data breaches, the situation was almost exactly reversed, with 57% of smaller companies impacted, compared to 33% of larger companies. All of the smaller companies have experienced at least one breach, while 13% of respondents at larger companies said they don't believe they've experienced a breach of any kind. Overall, those at the director level at larger companies are least aware of known breaches.

Assessing security awareness training

Leaders at the manager level and above recognize that not offering security awareness training represents substantial risk, and most offer an average of two to

Fig. 1: Types of Security Breaches Experienced



> **"C-level executives were twelve times more likely to be the target of social incidents and nine times more likely to be the target of social breaches than in years past."**

three types of training. Most recognize the value of continuous training, but few make it the top priority.

The top approach to security awareness—adopted by 67% of the respondents—focuses on the human element (sometimes referred to as the "human firewall") by trying to make employees aware of security risks and their role in detecting and stopping potential breaches.

There's little agreement, however, on the most effective method to create security awareness. Just 22% of those surveyed believe continuous training with regular follow-ups is the most effective, while more than half split their preferences almost evenly among creating engaging security training programs, using real-life hacking and phishing examples, and effectiveness monitoring and measurement.

Relatively few IT leaders indicate that they lack the necessary resources to implement security awareness training, such as technology, staffing, in-house skills, and funding. That raises the question of why security awareness programs in general tend to fall short in preventing breaches. Almost 60% of IT security practitioners saw an increase in employee phishing detection following security awareness training, according to one survey.

Fostering a culture of awareness

Security awareness training needs to be both continuous, to keep employees focused on threats and risks, and up to date, to keep pace with the evolving threat environment. The "human firewall" element is essential, but unless it's continually retuned and updated, the security awareness level will undoubtedly slacken.

Fostering a data protection culture to manage risks represents a cost-effective strategy that will help organizations overcome the persistent shortage and turnover of skilled security professionals. Employees who are constantly on the alert for the latest phishing attempts will be more likely to avoid those traps.

What's more, the commitment has to start at the top, and it's not just a matter of setting the tone for lower-level employees. According to Verizon's *2019 Data Breach Investigations Report*, "C-level executives were twelve times more likely to be the target of social incidents and nine times more likely to be the target of social breaches than in years past."

The methods to heighten organization-wide awareness and make it persistent aren't complicated, and they're certainly less expensive than the potential costs of breaches:

- Security awareness training that is continuous and evolves with the threat environment will keep employees alert.
- Educational emails serve as frequent reminders of threat tactics, and the potential costs of a breach.
- Simulated phishing can detect how employees are susceptible and expose weaknesses in the training regime.
- Positive feedback programs and low-cost incentives illustrate the importance that the organization places on the awareness effort, and on the participation of employees.

Constant awareness

Lax security practices and poor security awareness on the part of employees can result in security breaches that have serious consequences for organizations. Continuous learning is a powerful tool that every organization can tap to promote talent agility and career development in today's rapidly evolving workplace.