KnowBe4

6 Ways Security Awareness Training Empowers Human Risk Management

In the ever-expanding digital landscape, where cyber threats loom large, businesses are realizing that their greatest vulnerability often comes from within – their own employees.

Human error remains a significant factor in cybersecurity breaches, making it imperative for organizations to address human risk effectively. As a result, security awareness training (SAT) has emerged as a cornerstone in this endeavor because it offers a multifaceted approach to managing human risk.

Human Risk Management vs. Security Awareness Training: What's The Difference?

SAT and human risk management are closely related concepts but serve distinct purposes within the realm of cybersecurity.

SAT is a proactive approach taken by organizations to educate their workforce about cybersecurity threats and best practices. It aims to enhance employees' knowledge and skills, enabling them to recognize and mitigate potential risks effectively. Through training and simulated phishing email tests, employees learn to identify phishing attempts, understand secure data practices, and recognize social engineering tactics. The primary goal of SAT is to empower individuals, making them the organization's last line of defense against cyber threats.

Human risk management, on the other hand, encompasses a broader strategy. It involves not only the education and awareness aspects provided by security training but also the identification, assessment, and overall management of human-related vulnerabilities within an organization. Human risk management takes a holistic view, incorporating elements like policy enforcement, behavioral analysis, and ongoing monitoring to mitigate risks associated with employees' actions, both accidental and intentional. While SAT is a crucial component of human risk management, the latter involves a more comprehensive and strategic approach to managing the multifaceted aspects of human-related cybersecurity risks.

In an era where human error remains a significant cybersecurity risk, SAT fosters a vigilant workforce and empowers individuals to make informed decisions and identify suspicious activities, SAT significantly reduces the likelihood of breaches and data leaks. This proactive approach ensures that employees become active participants in the organization's security efforts, making it a pivotal element of human risk management. This proactive approach ensures that employees become active participants in the organization's security efforts, making it a pivotal element of human risk management.

Here are six ways SAT empowers organizations to more effectively manage human risk.

#1 Developing A Cybersecurity Mindset

SAT serves as the foundation upon which a robust cybersecurity mindset is built. By providing essential knowledge about phishing attacks, social engineering tactics, password hygiene, and safe browsing practices, employees are equipped with the necessary tools to recognize and combat potential threats. When armed with this awareness, individuals become a human firewall, questioning suspicious emails and attachments, thereby reducing the risk of falling victim to phishing attempts, and reducing the risk that cyberthreats pose to their organization.

#2 A Stronger Security Culture Via Company-Wide Vigilance

One of the most significant advantages of SAT lies in its ability to foster a culture of vigilance. Employees are not just passive recipients of information; they become active participants in safeguarding the organization. Through interactive training modules, real-life scenarios, and simulated phishing exercises, employees learn to identify red flags and report suspicious activities promptly to IT/infosec so threats can be mitigated in near real-time, before they have the chance to impact other employees. This heightened awareness creates a collective sense of responsibility, where everyone understands that cybersecurity is not just the IT department's concern but a shared responsibility that permeates every department and level within the organization.

#3 Mitigating Insider Threats

Insider threats, whether intentional or unintentional, pose a significant risk to businesses. SAT provides a nuanced approach to mitigating these threats. By educating employees about the importance of data confidentiality, the risks associated with oversharing on social media, and the consequences of negligent or malicious actions, organizations can build a culture of trust rooted in caution. Employees learn to recognize signs of insider threats, enabling early intervention and reducing the potential damage caused by malicious insiders.

#4 Enforcing Secure Data Best Practices

One of the primary goals of SAT is to instill secure data practices in employees' everyday routines. From handling customer data to managing internal communications, employees learn the importance of data encryption, secure file sharing, and the necessity of strong, unique passwords. By emphasizing the significance of secure data practices, organizations ensure that sensitive information remains protected, both within the digital realm and during offline interactions.

#5 Adapting to Evolving Threats

Cyber threats are dynamic, constantly evolving to bypass traditional security measures. SAT, however, evolves in tandem with these threats. Regular updates and continuous learning modules ensure that employees stay ahead of the curve, understanding the latest tactics employed by cybercriminals. By empowering employees with up-to-date knowledge and skills, organizations create a workforce capable of adapting to emerging threats. This adaptability proves invaluable in the face of ever-changing cybersecurity challenges, making SAT a proactive and responsive strategy for managing human risk effectively.

#6 Measure and Manage Risk

You can't manage what you don't measure, and human risk is no exception. Implementing a mature security awareness program and SAT platform allows organizations to model and report on risk, at the individual, department or organizational level. This means taking a data-driven approach to measuring security culture change and reduction of human risk.

By fostering a culture of vigilance, mitigating insider threats, enforcing secure data practices, and promoting continuous learning, organizations fortify their cyber defenses while reducing the risk cyber threats present to their organization from the inside out. In a digital age where a human error can cost millions of dollars, SAT bridges the knowledge gap and transforms employees into the organization's strongest asset in mitigating the risk of cyber threats.

LEARN MORE **About Strengthening Your Organization's Security Culture and Reduce Human Risk**

KnowBe4, Inc | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com