SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

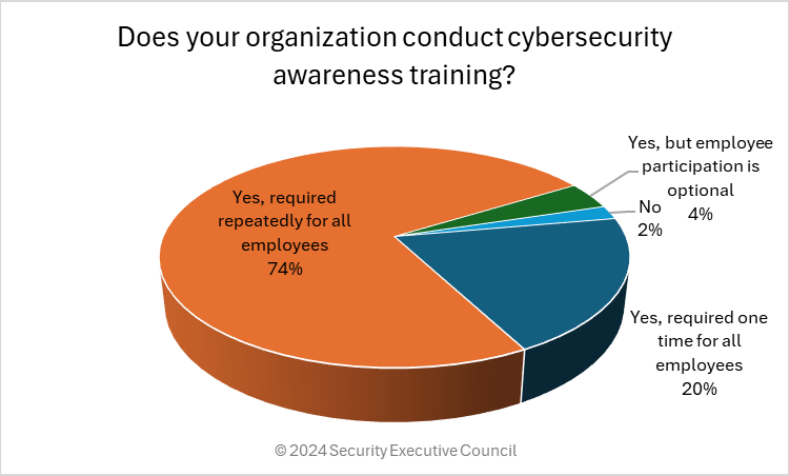
Program Best Practices > Info/Cyber Security >

Security Barometer: Essential Elements of Cybersecurity Awareness Training

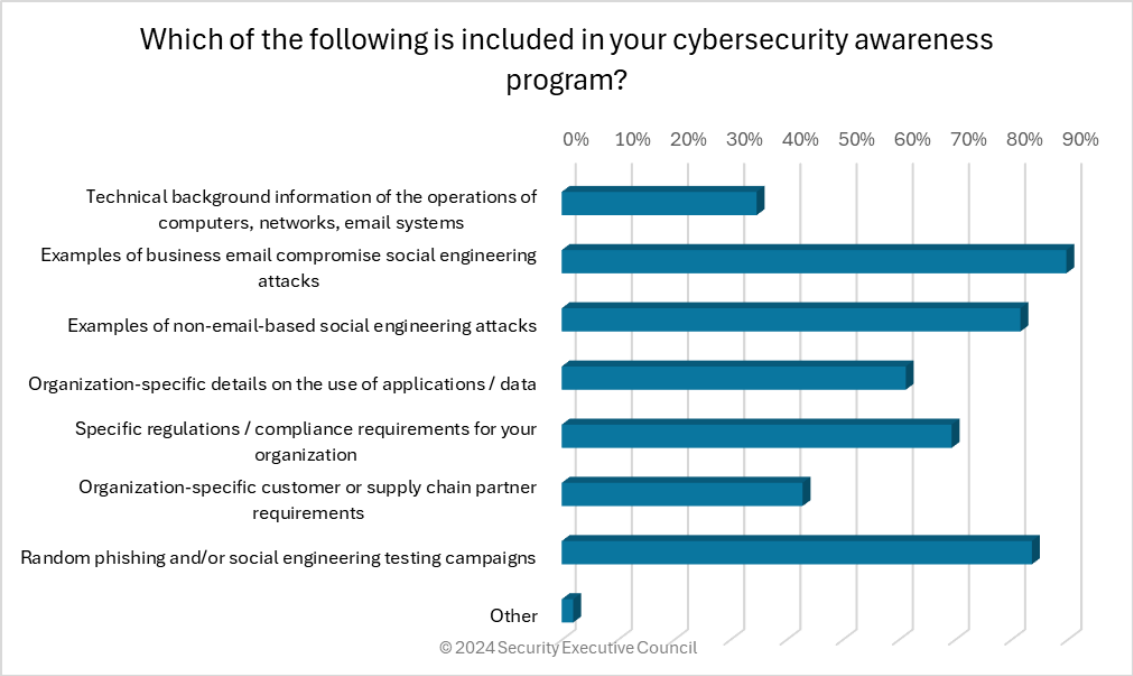
Information security is not just the job of infosec matter experts. Today's environment demands that all individuals play a role in protecting themselves and the organizations they work for.

Clearly, activities such as cybersecurity awareness training are meant to help protect organizations by informing individuals about how they can help prevent being used to cause damage.

This Security Barometer quick poll is capturing your peers' opinions on what makes up the essential elements of an effective cybersecurity awareness program.



Next question presented only to those who answered “Yes…” in the first question:



The “Other” answer was:

- 3rd party penetration audits

We asked survey participants, “What do you feel are the essential elements for an effective cybersecurity awareness program?” The responses proved enlightening, so we have provided some here. [Responses have been edited to protect the privacy of respondents and/or organizations.]

- Why security? What needs to be done? How this must be done? Monitoring and reviewing to ensure that they are being achieved, lessons learned
- 1) Engaging and Relevant Training, 2) Clear Communication and Reporting Guidelines, 3) Focus on Building a Security Culture, 4) Continuous Improvement and Updates.
- Since you are only as secure as your weakest target, identifying the user of threat vectors and how your users use this, i.e., email and targeting. Educating them, and keeping security at the forefront of their minds, is essential. Being that approximately > 80% percent of breaches involve the human element; it is most important to identify the users that fall susceptible to social engineering and train them to avoid these common attacks.
- Data Classification (Organization specific); Data Retention requirements; Explanations of Material changes in technology; Explanations of current scams & threats.
- Threats, awareness, risk management, and training.
- Real life examples and continually updating.
- I think what is essential is an anti-malware and firewall, communication and training how to care for the equipment, how access to public internet and how care for your privacy information.
- It needs to be fit the organizational environment and like any other program it is not a one time event, its ongoing, personalized and measured.
- Making the program fast and efficient, otherwise, compliance falls off sharply.
- It's all about keeping your data protected and any organization needs to have some kind of data management in place to secure data. Employees need to be aware of any security breach attacks and it is important that the organization keeps them up to date on processes and procedures.
- I think instructor led training with question/answer is more effective for some people, however cost could be an issue. Also important is how does this training help them in their personal family digital awareness (children and elderly), as cybercrime is more than attacking business.
- A cybersecurity awareness program should go beyond traditional methods by incorporating gamification elements, such as interactive challenges, leaderboards, and rewards for participation and achievement. It also leverages storytelling techniques to make complex concepts more relatable and memorable, using real-life scenarios and examples to illustrate the importance of cybersecurity in employees’ daily lives.
- As a small services provider, we have fallen into the trap of not taking the time to address the issue as we have false comfort in knowing with whom we are working with day to day. We need to do more...
- Initial awareness. Continuing training. Random testing.
- Security Awareness training for contractors is part of their agreement to complete.

- Repeated training, random testing, and ownership of the program by trained professionals with clear job duties, guidelines and parameters.
- Training needs to be relevant and engaging. I find introducing guidance that employees can use both on the job and in their private lives is received better.
- Continuous changing up of awareness so people don't just "check the box". Real life scenarios.
- Cyber security awareness must be integrated with the general practice of IT tech management and tech "hygiene". A practical example: Phishing "click tests" are pointless when the business constantly sends out new links etc., that staff must click.
- Compliancy and making sure the information provided is relative to them and their particular function within the business."

Visit the Security Executive Council web site to view more resources in the Program Best Practices : Info/Cyber Security series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

