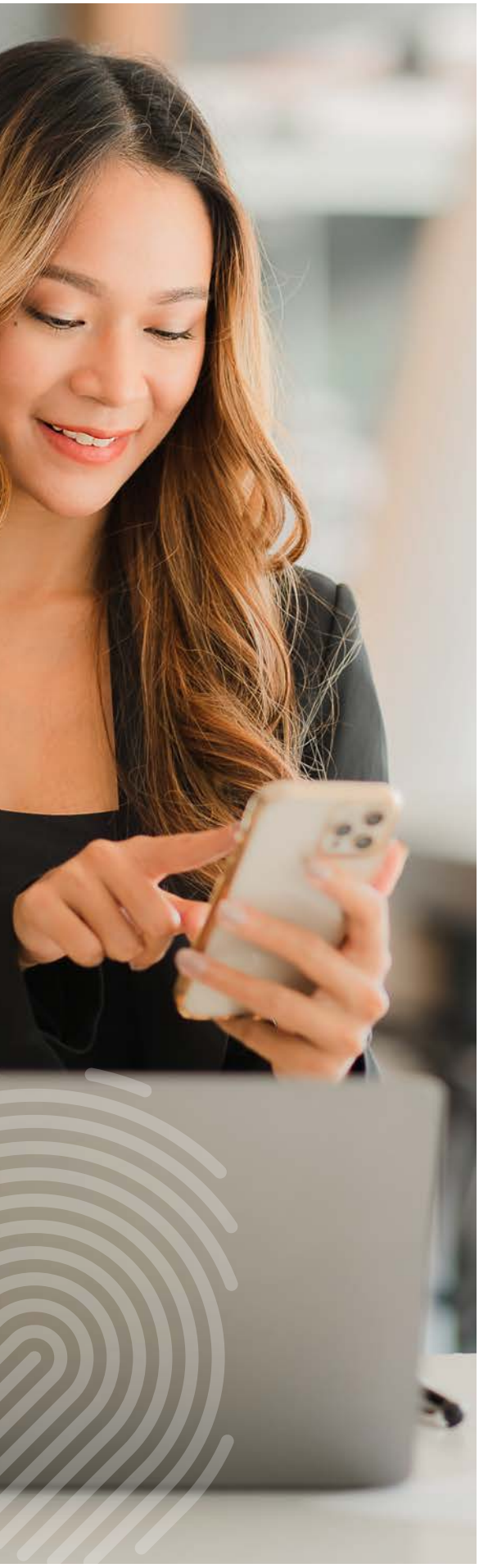
SECURING
THE HUMAN LAYER

How to Make Insiders Your Defense Allies and Influence Behaviors

H LAYER™
CREDENTIALING



Contents

Changing Human Behaviors in the Era of Human-Centric Threats

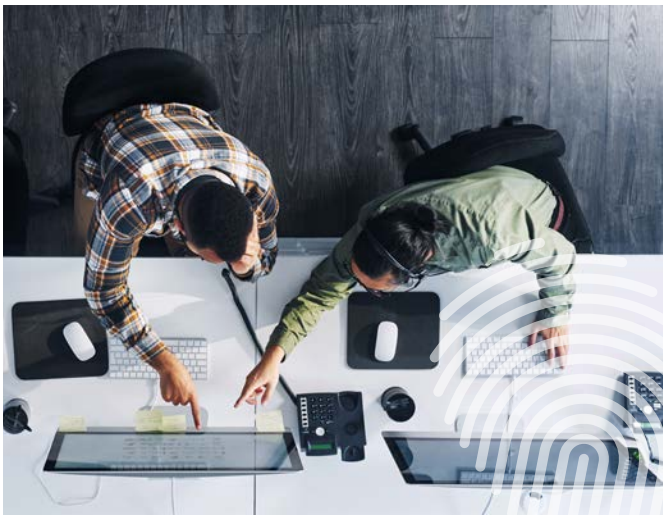
The proliferation of cyber threats drives organizations to harden their defenses continuously and improve security tools. But threat actors move fast to adapt to these changes. As defensive technologies mature, attackers continue to fixate on the human factor as the weaker link.

Aided by emerging tools like artificial intelligence (AI), cybercriminals are exploiting human errors and behaviors to compromise organizations in both true-and-tried and novel ways. In this era of rising human-centric threats, a strong culture of security is paramount. Security awareness and training programs lay the foundation for security culture.

Gartner named security behavior and culture programs the second most significant trend in IT infrastructure and operations for 2025,[1] stating that security programs must evolve to address both behaviors and culture. In other words, protecting your IT infrastructure requires addressing unsafe behaviors within your organization and nurturing a security-first mindset.

More than simply a way to defend your organization, your security culture can be a competitive differentiator — empowering you to innovate safely and confidently and drive business growth.

This e-book discusses the impact of the human factor on your organization's cybersecurity. It also provides practical advice on implementing and maturing a security awareness and training program.



Protecting your IT infrastructure requires addressing unsafe behaviors within your organization and nurturing a security-first mindset.

Threat Actors Adapt to the New Landscape

Our expanding digital lives have increased the role of digital identities in recent years — driving a shift in threat actors' tactics. Security researchers observed a four-times rise in identity attacks in 2024,[2] partly due to attackers' increased focus on identities. At the same time, the proliferation of digital tools like collaboration and communication apps and social media platforms provides threat actors with many new channels for "hacking" humans.

One example of a growing identity-centric threat is the adversary-in-the-middle phishing attack. In response to widespread multi-factor authentication (MFA) adoption, cybercriminals are circumventing controls by tricking individuals into clicking a link that completes the MFA step for them. Last year, these types of attacks grew 146%, according to Microsoft researchers.[4]

Even as tactics evolve, phishing and social engineering remain as prevalent as ever and are on the rise. Social engineering — especially email phishing, voice phishing (vishing), and SMS phishing (smishing) — is the primary initial attack vector for everything from ransomware attacks and malware distribution to business email compromise (BEC). And 84% of IT leaders say they're observing an increase in phishing volume, sophistication, or both.[5]

9 out of 10 surveyed organizations said they experienced a successful identity-related breach due to phishing or vishing in the past 12 months.[3]

Prevalence of Phishing Threats

The number of surveyed users and security professionals who report experiencing phishing in the past 12 months[6]

The thriving cybercrime-as-a-service ecosystem makes it easy for malicious actors to conduct social engineering and phishing campaigns with limited technical skills. Easily accessible and inexpensive generative AI tools further remove their barriers to success, lowering the cost and improving the effectiveness of these attacks.

Organizational leaders are aware of this emerging risk:

62%

of surveyed leaders believe their employees will be successfully attacked due to malicious actors' use of AI tools.[7]

40%

of surveyed security decision-makers expect to see AI-powered phishing threats in the following year.[8]

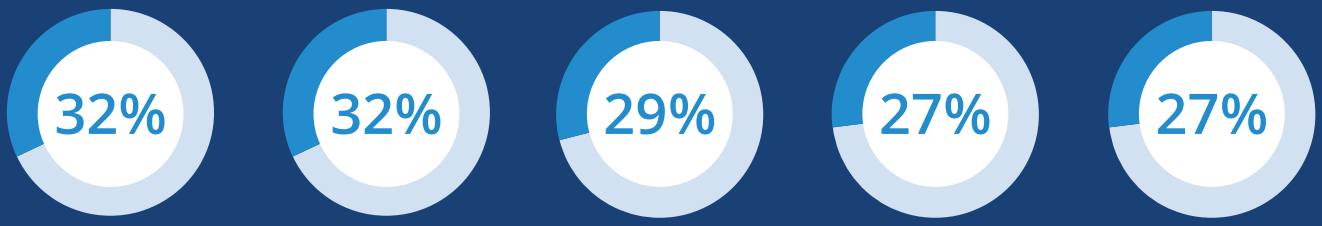
A security-first culture can help translate this awareness into action.

The Escalating Cost to Your Organization

Social engineering and phishing attacks can result in tremendous financial losses to organizations. Data breaches caused by these two vectors are among the costliest: $4.88 million per breach on average for phishing and $4.77 million for social engineering.[9]

It takes just under a minute for someone to fall for a phishing scheme,[10] yet identifying and containing breaches stemming from phishing and social engineering takes months (261 and 257 days, respectively).[11] This wide-open window gives attackers ample time to inflict damage to your organization.

The most considerable consequences of phishing attacks (based on the percentage of surveyed organizations that have experienced them):[12]



Loss of intellectual property or other data

Ransomware infection

Customer data breach

Credential or account compromise

Reputational damage

These trends underscore the need to fortify your human layer. This is where a security-first culture and a holistic security awareness and training program come in.

The Role of Security Culture in Protecting Your Organization

A strong security culture mitigates human risk by addressing human error, promoting and reinforcing proactive and positive behaviors, and empowering employees to protect your organization actively. By nurturing a security-first culture, you make cybersecurity a shared priority across your organization rather than solely your IT team's responsibility. You also turn employees from a weak link into your best ally in defending against cyber threats.

Embedding security culture in your core values and day-to-day operations can drive lasting change, improve behaviors, and boost organizational resilience. Implementing an employee awareness and training program is foundational to achieving these outcomes.

Organizations recognize the importance of these programs for employees:

97%

of surveyed leaders believe more training and awareness can help reduce cyberattacks.[14]

54%

of surveyed chief information security officers (CISOs) say this area is a priority for their IT departments in the next two years.[15]

Organizations that nurture a security culture report a 46% boost in security resilience.[13]

Data shows that security awareness and training programs effectively reduce human risk. KnowBe4 found that employees participating in phishing security tests are better at detecting simulated phishing campaigns than those who did not — and the more frequent the training, the better their performance.[16]

"Security awareness training is a big part of human risk management, but security culture is more than just training. You're trying to change how people behave and feel about security."

– Roger A. Grimes, KnowBe4 data-driven defense evangelist, author of 15 books on cybersecurity

Security Culture 101

Security culture is typically defined as the shared values, attitudes, behaviors, and actions that shape how an organization thinks about and approaches cybersecurity. Common attributes of a security-conscious culture include:

- **Shared responsibility**
  Everyone, from leaders to frontline employees, plays a role in maintaining security.
- **Leadership commitment**
  Decision-makers demonstrate that security is a business priority.
- **Employee empowerment**
  Employees have the knowledge and tools to protect the business while staying productive.
- **Effective communication**
  Open communication related to security goals and risks is encouraged and modeled across the organization.
- **Continuous awareness and training**
  Employees receive ongoing education about best practices and the threats their organization faces.

The Core Components of an Awareness and Training Program

Your training program may look different depending on whether you're just starting or have been growing it. The following components are core to ensuring an effective and sustainable endeavor:

Organizational and leadership support: Your organization's leaders set the tone for the security culture, and their buy-in is essential before getting the rest of the organization on board. Not only do you need the leaders to dedicate resources to the program, but the program will be more successful if they model security-conscious behaviors.

A defined security awareness strategy: This is a policy document that outlines aspects such as the program's goals and objectives, business needs, security threats that you want to mitigate, and ramifications when employees don't comply.

Tailored training content and delivery: This includes the audience, content format, delivery mechanism, frequency, and cadence. You need to tailor the content to specific audiences (e.g., based on location, roles, and responsibilities). Some roles, like C-suite executives, finance teams, and other privileged users, may require additional training.

Communication activities: Your program's success relies on continuous communication and employee engagement. Using various methods, from distributing newsletters and reminders to celebrating success during all-hands meetings, keeps the topic of security fresh in employees' minds.

Simulations and testing: Tools like simulated phishing and tabletop exercises can test employee responses to threats while establishing a baseline. These tools can also identify areas for additional training and measure the effectiveness of specific program areas.

Metrics and assessments: Identifying other metrics, both quantitative and qualitative, will help determine how well the program is working and pinpoint areas for potential improvement.

Monitoring and reporting: Your leaders will want to know the program's impact on the organization and evaluate the return on investment. Assessing the effectiveness of your efforts and reporting outcomes to different stakeholders (e.g., department leads, upper management, auditors) also helps you stay on track with the program's objectives.

"You need the CEO and senior management to embrace security culture. The best programs I've seen have the CEO kicking off the annual security awareness training meeting and talking about its importance."

– Roger A. Grimes, KnowBe4 data-driven defense evangelist, author of 15 books on cybersecurity

Implementing and Maturing Your Security Awareness Initiative

Many organizations have some form of a security awareness and training program. However, employees may not see the value of this training — 43% of those surveyed said they would go to great lengths to avoid security training, trading a session for things like a root canal or rush-hour traffic.[17]

This data indicates that security programs are ineffective if they fail to engage or resonate with employees. People tune out when the training feels like a burden. If you want your effort to drive lasting change, the training program needs to earn employee buy-in, connect with real-world behavior, and feel relevant to everyone, from interns to executives.

10 Steps to Creating and Launching a Program

1

Get the leadership on board.

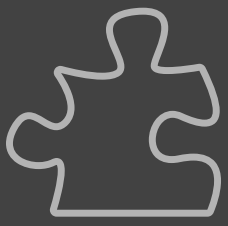
As noted earlier, you need the leadership by your side. Build the case for your initiative with immediate leaders like your manager or director. Then, expand to key figures like executives (e.g., chief risk officer) and business decision-makers. Prepare to discuss the need for a program, the potential impact, and the resources that may be required, including a budget. Speak the leaders' language — avoid technical jargon and tie the outcomes to business goals and objectives.

Establish the need.

You'll need to understand the gap between employees' existing knowledge or skills and desired state. Techniques include reviewing existing risk assessments, conducting a needs assessment, and analyzing operational risks for different audiences.

2

3



Determine engagement strategies.

Tactics like gamification, rewards, and incentives will make participation more compelling. Figure out what employees may respond best to, whether that's prize giveaways, food, or friendly competition among teams. Other effective practices include storytelling (examples of real-world attacks), case studies (anonymized examples within your organization), milestone celebrations, and informal sessions with security ambassadors.

Design the program.

Develop the details of your training strategy and policies, such as scope, goals, risk-based objectives, roles and responsibilities, training formats and frequency, expected behaviors, rewards and consequences, and metrics.

4

5

Gather input from stakeholders.

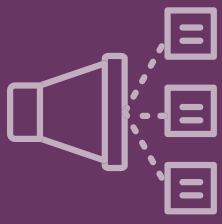
When you have a general idea of the program, get feedback from various teams, departments, and individuals in roles related to specific training areas. Their input will help uncover any incorrect assumptions you may have about different business units' processes and workflows that will affect the training content or efficacy.

Create compelling content.

Some people learn better by watching a video or interacting with a self-paced module, while others prefer face-to-face instruction. Providing as many formats as possible will help ensure that the security message reaches a broader audience.

6

7



Communicate before rollout.

Announce the initiative early and clearly to all stakeholders using multiple channels such as email, collaboration apps, company newsletters, and meetings. Explain the program's importance, goals, and employee expectations. Provide mechanisms for employees to ask questions and offer feedback.

Schedule launch activities.

Roll out the program and schedule sessions and activities according to your selected frequency and cadence. Continue to communicate updates and reminders. Additionally, integrate training activities into new employee onboarding.

8

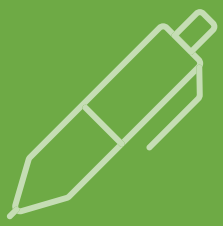
9

Monitor progress and measure outcomes.

Track the progress of your implementation and use metrics to assess changes in behavior. Review qualitative data, such as informal employee feedback about the program and content, as you evaluate effectiveness.

Review and revise regularly.

Review your program on a consistent schedule, such as annually, to ensure it continues to meet goals and objectives and that the content reflects your current risks and threat landscape. Incorporate lessons learned throughout the year from program delivery, metrics, and other activities that can help improve your efforts and program outcomes.



10

"The best plans and programs I've seen get into version 5, 6, or 7 because they're being refined and reviewed by the people who will be impacted the most."

— Marc Vasquez, former cyber regional training and exercise specialist, Cybersecurity and Infrastructure Security Agency (CISA)

Helpful Resources

- NIST, Special Publication 800 | Building a Cybersecurity and Privacy Learning Program
- KnowBe4, Example Security Awareness Training Policy Guide
- SaltyCloud, Growing an Information Security Culture, Complete Guide
- KnowBe4, The Ultimate Guide to Security Awareness Training

Continuously Maturing Your Program

Threats evolve, business needs change, and emerging technologies introduce new risks. Both the threat and the business environments are dynamic, and your program needs to adapt. Even a well-established program has areas that can be improved and fine-tuned.

Consistently maturing your security awareness program helps strengthen your security culture and harden your human layer.

KnowBe4 has established a maturity scale for security culture, and you can adapt this framework to your training program. This model has five maturity levels:[18]

Program Maturing

Level	Activities	Primary goal
Basic compliance	Bare minimum training and limited metrics	Checking a compliance box
Security awareness foundation	Training conducted during employee onboarding and at least every year thereafter and includes occasional phishing simulation	Providing diverse content
Programmatic security awareness and behavior	A more intentional program that includes integrated tools and quarterly training with simulations	Encouraging security-aware behaviors
Security behavior management	Continuous training, tailored to different audiences and delivered through various methods	Driving behavioral change
Sustainable security culture	Intentionally measure, influence, and reinforce security culture using multiple methods	Making security part of the organization's fabric

Recruiting Cybersecurity Champions

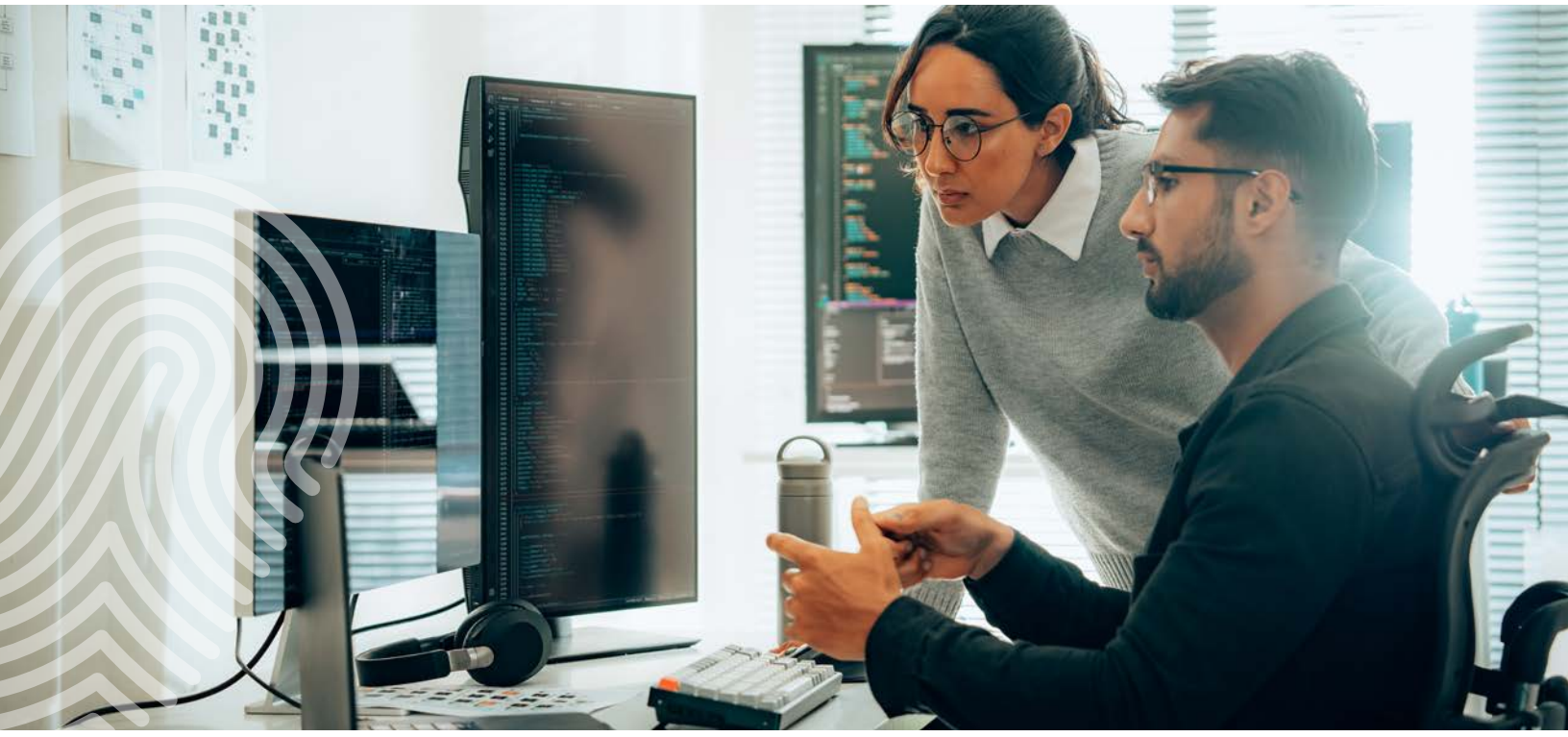
One way to scale security awareness is through a security champions or ambassadors program. This effort can be formal or informal, but typically, it's more successful when formalized.

Security champions are cheerleaders for security culture and best practices whose roles are outside of your IT or security team. They are peers who are passionate about security and bring a perspective that's different from the technical experts' lens.

Champions can serve several roles:

- Provide the link between the IT or security department and other teams.
- Drive informal conversations that promote a security culture.
- Model good security behaviors and educate their peers.
- Offer feedback on proposed changes to security policy and procedures.
- Facilitate knowledge-sharing activities.

Security culture is typically top-down, whereas security champions add a bottom-up approach.



"An important aspect of a security awareness program is to get to the point where you are helping others promote security for you. That's where security awareness ambassadors can help in various ways."

— Marc Vasquez, former cyber regional training and exercise specialist, CISA

The Value of Certification Programs

Certifications like the Security Awareness and Culture Professional (SACP) credential prepare individuals interested in security culture for developing, implementing, and managing a security awareness and training program at their organization. These certifications are a valuable resource that provides professionals with knowledge and insights into best practices in security awareness.

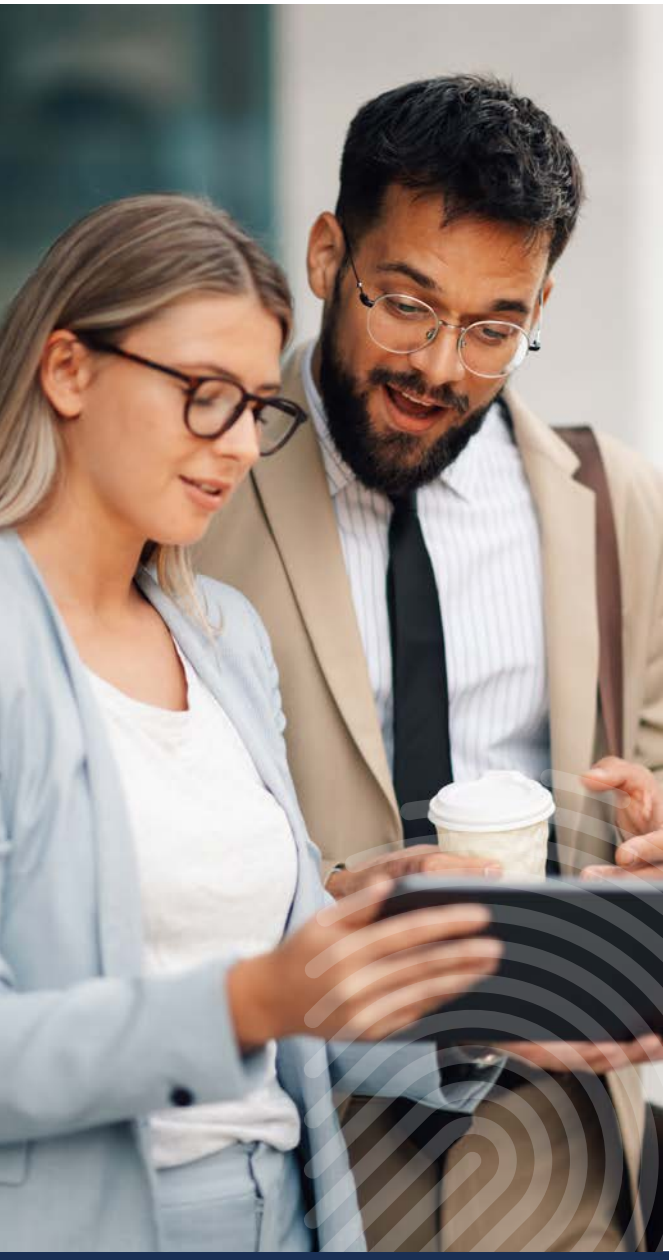
For professionals, a certification can:

- Help advance or launch a career in security awareness and grow technical skills.
- Identify knowledge gaps and learn new aspects of security awareness programs.
- Tap into a community of peers who can share insights and strategies.

For organizations, the certification:

- Validates an individual's competence in various areas, such as program design and assessment.
- Demonstrates the person's dedication to professional development and security best practices.
- Creates a competitive advantage by showing potential customers the organization's commitment to security.

SACP is the only vendor-neutral certificate focused on security awareness and culture. Developed based on a comprehensive job task analysis and input from industry experts, the SACP exam covers seven core aspects, both business and technical, of developing, implementing, and monitoring a security awareness program.



Final Thoughts

Cybercriminals will not cease their attacks on the human layer any time soon. Your insiders, however, are not just your most significant risk — they're your best asset. A security-aware culture with informed, engaged, and proactive employees is a formidable defense against threat actors.

Like technology, hardening the human layer takes a thoughtful strategy and practical tools. Building a sustainable security awareness and training program is how you turn employees into empowered security allies — and your human layer into a lasting line of defense.

Become a recognized leader in security awareness and culture — learn about the SACP credential.

Sources Cited

1. Gartner, "Gartner Identifies the Top Trends Impacting Infrastructure and Operations for 2025," December 2024.
2. Red Canary, "Identity attacks and infostealers dominate the 2025 Threat Detection Report," March 2025.
3. CyberArk, "Identity Security Threat Landscape Report," 2024.
4. Microsoft, "Microsoft Digital Defense Report 2024," October 2024.
5. Dashlane, "New Data Shows Impact of AI-Powered Phishing on Businesses," April 2025.
6. Proofpoint, "State of the Phish," February 2024.
7. Fortinet Training Institute, "2024 Security Awareness and Training Global Research Report," October 2024.
8. CyberArk, "Identity Security Threat Landscape Report," 2024.
9. IBM, "Cost of a Data Breach Report," 2024.
10. Verizon, "2024 Data Breach Investigations Report," 2024.
11. IBM, "Cost of a Data Breach Report," 2024.
12. Proofpoint, "State of the Phish," February 2024.
13. Cisco, "Security Outcomes Report, Volume 3," January 2023.
14. Fortinet Training Institute, "2024 Security Awareness and Training Global Research Report," October 2024.
15. Proofpoint, "2024 Voice of the CISO," May 2024.
16. KnowBe4, "Data Confirms Value of Security Awareness Training and Simulated Phishing," 2023
17. Dashlane, "The State of Credential Security," March 2025.
18. KnowBe4, "Introducing the Security Culture Maturity Model," 2022.