CROWDSTRIKE
business resilience

Best Practices

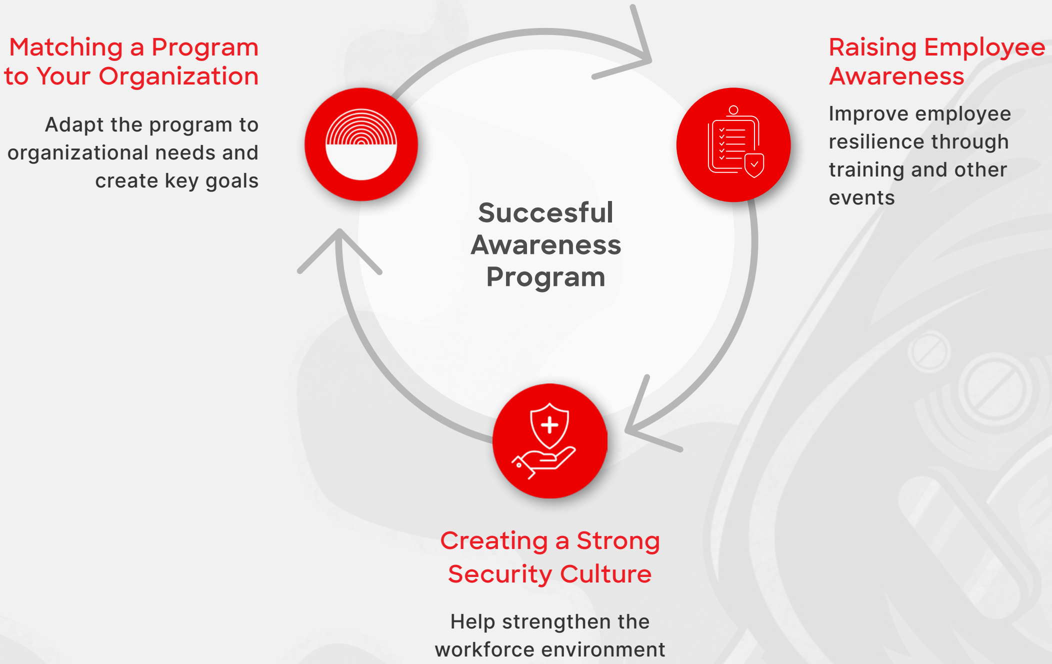
Building Your Own Security Awareness Program

CrowdStrike's Approach

A security awareness program is pivotal to the success of any organization. Successfully running and implementing the program in an organization's environment helps improve employees' resilience against adversaries. In today's age of prevalent social engineering attacks, an effective security awareness program empowers employees to understand current and future threats.

This guide will help you structure a security awareness program for your own company on a scale that will work for you. In addition to the structural recommendations in this document, additional resources on key topics are available for you to use at your own discretion, sharing them with your organization as you see fit. The best practices in these resources are based on the most important points in CrowdStrike's own Security Awareness program.

To run a successful awareness program, organizations should consider following the three stages of implementation:



Matching a Program to Your Organization

Adapt the program to organizational needs and create key goals

Raising Employee Awareness

Improve employee resilience through training and other events

Creating a Strong Security Culture

Help strengthen the workforce environment

Aligning the Program to Your Organization

The first step in creating your security awareness program is to outline key objectives with the leadership team that align with company goals and guidelines. Your program will require constant interaction across your organization — foster a great relationship with the leadership team and choose a champion to help enforce actions that support the program. Your champion can reach your organization in ways that you cannot.

Key Points to Focus On:

- Consult with the legal or audit and compliance team to align the program with policies and regulations
  - Policy acknowledgement may be required to prove whether an employee has read and agreed to the assigned policies
- Promote your program to build upon existing resources
  - Adopt a program slogan or logo
  - Locate and assess existing work
  - Set aside a budget for gifts or rewards
- Keep track of metrics for audit/HR purposes

Raising Employee Awareness

Remember, your program must reach everyone in your organization regardless of their role. Employees with or without a cyber background have to keep company data safe so that your organization can operate securely. It is critical to build a vigilant workforce.

Key Points to Focus On:

- Look for the best ways to reach your workforce
  - Create an annual training program
  - Implement a phishing exercise program
  - Encourage end user reporting, conduct new hire trainings and recognize Cybersecurity Awareness Month (CSAM)
- Implement a role-based training program for employees within the organization based on regulatory requirements (e.g., NIST Special Publication 800-16)
- Consult with the threat and incident response team to identify current advanced persistent threats (APTs)
  - Check with the incident response team for clearance before sharing information about APTs
- Assist with human resources issues if necessary
- Report to leadership on completion rates for mandatory security training

Creating a Strong Security Culture

One way to keep the workplace secure is by having security-conscious employees. Having a strong security culture unites all employees and departments, ensuring they all follow the same standards.

Key Points to Focus On:

Vendor Utilization

Vendors are great resources for the awareness program because their dedicated teams create resource materials related to cybersecurity.

- Subscription-based training vendors
- Free training vendors
  - SANS, CISA

Reward System

Rewarding employees with gifts for taking time from work to interact with the security awareness program can help make them enthusiastic about the program content.

Promote the Program

Use various means of communication.

- Develop websites, social media, training, games, emails, webinars, articles and newsletters
- Organize fun events or activities based on cyber awareness holidays
- Communicate more during national Cybersecurity Awareness Month (October)
- Create and promote cyber content that can be shared outside your organization with family members, friends and social circles (clubs/schools)

Get more resources from CrowdStrike for creating your own Security Awareness Program →

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.