MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program

SSAP
Secururity Awareness Professional
giac.org/ssap

2 Day Course	12 CPEs	Laptop Not Needed

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their workforce. As a result, people, not technology, have become the most common target for cyber attackers. The most effective way to secure the human element is to establish a mature security awareness program that goes beyond just compliance, changes peoples' behaviors and ultimately creates a secure culture. This intense two-day course will teach you the key concepts and skills needed to do just that, and is designed for those establishing a new program or wanting to improve an existing one. Course content is based on lessons learned from hundreds of security awareness programs from around the world. In addition, you will learn not only from your instructor, but from extensive interaction with your peers. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

You Will Learn

- The Security Awareness Maturity Model and how to leverage it as the roadmap for your awareness program
- How to gain and maintain leadership support for your program
- Key models for learning theory, behavioral change and cultural analysis
- How to identify different target groups and deploy role based training.
- How to effectively engage and communicate to your workforce, to include addressing the challenges of different roles, generations and nationalities
- How to sustain your security awareness program long term, including advanced programs such as gamification and ambassador programs
- How to measure the impact of your awareness program, track reduction in human risk, and communicate the program's value to leadership

Who Should Attend

- Security awareness / communication officers
- Chief Security Officers, Risk Officers and security management officials
- Security auditors, and governance, legal, privacy or compliance officers
- Training, human resources and communications staff
- Representatives from organizations regulated by industries such as HIPAA, GDPR, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, or any other compliance-driven standard
- Anyone involved in planning, deploying or maintaining a security education, training or communications program

Section Descriptions

SECTION 1: Plan and Build

TOPICS:

- The five stages of the Security Awareness Maturity Model
- The three variables of risk and their role in awareness
- Why humans are so vulnerable and the latest methods cyber attackers use to exploit these vulnerabilities
- The learning continuum: awareness, training, and education
- Steps to gaining and maintaining leadership support
- How to develop and leverage an effective Advisory Board
- B.J. Fogg Behavior Model and how it applies to your overall strategy of changing workforce behavior
- Developing a strategic plan based on three key questions: Who, What, and How
- Who: Identifying the different targets of your awareness program. Whose behaviors do you want to change? NOTE: This section includes an interactive group lab where you identify and analyze key target groups in your organization
- What: Identifying and prioritizing the top human risks to your organization and the behaviors that will most effectively manage those risks. NOTE: This section includes two interactive labs, one conducting a qualitative risk analysis for your organization and a second lab on behavioral management by defining key learning objectives

SECTION 2: Implement, Maintain and Measure

TOPICS:

- How: How will you communicate your program and train your workforce. This includes defining why cybersecurity is important to your organization, different training modalities and the most successful strategies to engage people.
- The effective use of imagery, to include imagery within diverse or international environments
- Top tips for effective translation / localization
- The two different communication methods: primary and reinforcement, and the advantages / disadvantages of each
- How to effectively develop and provide instructor-led training (ILT)
- How to effectively develop and deploy online / computer based training (CBT)
- Different reinforcement methods, including newsletters, fact sheets, posters, internal social media, hosted speaker events, hacking demos, escape rooms, lunch-n-learns and numerous other training activities. NOTE: This section includes an interactive lab combining a cultural analysis, communication methods, and different training modalities
- Long term sustainment for effective culture impact, to include gamification and ambassador programs
- Design, deploy, and leverage metrics to measure the impact of your awareness program, including how to effectively establish a global phishing program and measure culture. Note: This section includes an interactive lab in identifying and defining the top security awareness metrics specific to your program.
- Walking through the final planning and execution steps, to include documenting a comprehensive project plan

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast