MGT433: Managing Human Risk: Mature Security Awareness Programs

SSAP
Secururity Awareness Professional
giac.org/ssap

2 Day Course	12 CPEs	Laptop Not Needed

This Course Will Prepare You to:

- Understand the Security Awareness Maturity Model and how to leverage it as the roadmap for your awareness program
- Gain and maintain leadership support for your program, including aligning the program with your organization's strategic priorities
- Implement key models for learning theory, behavioral change, and cultural analysis
- Explain the difference between awareness, education, and training
- Identify the maturity level of your existing awareness program and the steps to take it to the next level
- Ensure compliance with key standards and regulations
- Define human risk and explain the three different variables that constitute it
- Explain risk assessment processes
- Leverage the latest in Cyber Threat Intelligence and describe the most common tactics, techniques, and procedures used in today's human-based attacks
- Identify, measure, and prioritize your human risks and define the behaviors that manage those risks
- Define and build a role-based training program to manage your organization's human risks
- Effectively engage, train, and communicate with your workforce, including by addressing the challenges of different cultures, generations, and nationalities
- Sustain your security awareness program over the long term, going beyond changing behavior to changing culture
- Measure the impact of your awareness program, track reduction in human risk, and communicate the program's value to leadership

"Lance is a great speaker. I love the charisma, the energy, and the banter."

— Chris Cioffi, **Western Power Distribution**

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.

What You Will Receive

This course provides you with the opportunity to join the SANS Security Awareness Community Forum, a private, invitation-only community of over 1,500 awareness officers who share resources and lessons learned. In addition, you will receive the following with the course:

- Printed + Electronic course books that include slides with detailed notes for each slide
- Printed + Electronic lab book
- Digital download package containing digital copies of all the labs, supplemental materials, reports, and examples
- MP3 audio files of the complete course lecture
- One 90-day license to the entire SSA library of content. Read the FAQ here.

Additional Resources

For those of you who are looking to get involved in this field, or are already involved but looking to grow, consider reading this blog on how to develop your career path.

Author Statement

"Having been actively involved in information security for more than 20 years, I have seen one constant factor: people are the number one attack vector for cyber attackers because we fail to properly invest in people and secure them. Once trained, your workforce will become your greatest asset, not only to prevent incidents but also to quickly identify and report them, resulting in a far more resilient organization. I am extremely excited about MGT433, as it provides organizations with the skills, resources, and community they need to build a mature security awareness program that effectively manages and measures human risk."

— Lance Spitzner

Section Descriptions

SECTION 1: Fundamentals and Identifying/ Prioritizing Human Risk

The first course section begins with the fundamentals by specifically answering two questions: What is awareness and how do we define it? What is human risk and how can awareness programs enable us to effectively manage it? We then cover the most critical foundations for a successful program, which include leadership support, a program charter, and an advisory board. We'll cover the science of behavior change and the two pillars of a strategy that supports that change. We then do a deep dive into identifying and prioritizing your organization's top human risks and the behaviors to manage those risks.

TOPICS:

- The five stages of the Security Awareness Maturity Model
- The learning continuum: awareness, training, and education
- The definition of human risk and the three variables that define it
- Why humans are so vulnerable and the latest methods cyber attackers use to exploit these vulnerabilities
- Steps to gain and maintain leadership support for your program
- How to develop and leverage an effective Advisory Board
- The B.J. Fogg Behavior Model and how it applies to your overall strategy of changing workforce behavior
- Developing a strategic plan that prioritizes your organization's human risk and the behaviors to manage those risks, and that enables changing those behaviors.
- A walk-through on how to conduct a human risk assessment and how to prioritize your organization's top human risks, including leveraging the latest in Cyber Threat Intelligence (CTI): NOTE: This section includes two interactive labs. In the first lab you will analyze a CTI report and identify the most common risks to your industry. In the second lab, you will identify the top three human risks to your organization.
- An analysis of how to identify and prioritize the key behaviors that manage your organization's top human risks, including an overview of learning objectives. NOTE: This section includes an interactive lab on defining the key behaviors to manage a specific human risk.

SECTION 2: Implementing and Measuring Change

The second course section begins with how to change behaviors at an organizational level, with a focus on building a customized engagement strategy unique to your organization's structure and culture. We then go into the different outreach and training categories and modalities before transitioning into a look at how to sustain change over the long term and impact culture. Finally, we'll explore how to measure the impact of your program and communicate that impact to leadership. We finish the section with a focus on how to put this all together and effectively implement your program.

TOPICS:

- Introduction of the Golden Circle and the importance of "why"
- How you can effectively create an engagement strategy leveraging the AIDA marketing model
- Elements of cultural analysis
- Top tips for effective translation and localization
- The effective use of imagery, with a focus on diverse or international environments
- The two different training categories, primary and reinforcement, and the roles of each
- How to effectively develop and provide instructor-led training (ILT)
- How to effectively develop and provide virtual live training (VLT)
- How to effectively develop and deploy computer-based training (CBT)
- Different reinforcement methods, including newsletters, fact sheets, posters, internal social media, hosted speaker events, hacking demos, scavenger hunts, virtual lunch-and-learns, and numerous other training activities. NOTE: This section includes an interactive lab challenging you to conduct a cultural analysis of your organization and develop a customized engagement strategy.
- Sustaining an effective culture impact over the long term
- How to design, deploy, and leverage metrics to measure the impact of your awareness program
- Walk-through of the final planning and execution steps, including documenting a comprehensive project plan

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

SSAP
Secururity Awareness Professional
giac.org/ssap

SANS Security Awareness Professional

The SANS SSAP credential signifies, documents, and certifies that the holder possesses the expertise and skills to effectively manage and measure human risk. These professionals are responsible for elevating the overall security behavior of the workforce through the use of effective ongoing learning programs.

Areas Covered:

- Five stages of the Security Awareness Maturity Model
- Impact measurement and communication of awareness program performance
- Key models for learning theory, behavioral change, and cultural analysis

"Soup to nuts, this course covers the entire designing, building, deploying and measuring of an effective security awareness program."

— Chris Sorensen, **GE Capital**