MGT433: Managing Human Risk: Mature Security Awareness Programs

People are the primary attack vector. Manage your human risk.

Learn the key lessons and the roadmap to build a mature awareness program that your workforce will love and that has an impact you can measure. Apply models such as the BJ Fogg Behavior Model, AIDA Marketing funnel, and Golden Circle, and learn about the Elephant vs. the Rider.

The course content is based on lessons learned from hundreds of security awareness programs from around the world. 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 plan to implement as soon as you return to your organization.

Business Takeaways:

• Align your security awareness program with your organization’s strategic security priorities
• Effectively identify, prioritize and manage your organization’s top human risks.
• More closely integrate your security awareness efforts with your security team’s overall risk management efforts.
• Make the most of your investment by sustaining your security awareness program long term, going beyond changing behavior to changing culture

Hands-On Training:

A big part of the course is not only learning but applying what you learn working as groups with your peers. Not only does this provide you a far better understanding and application of course content, but enables you to interact and learn from others. This two-day course has five labs. Each lab is approximately 20–30 minutes to complete as a team, with another 20–30 minutes of group discussion, for a total time of three to four hours.

• Lab 1: Read, analyze and identify the top human risks based on the Verizon Data Breach Investigations Report
• Lab 2: Review, identify and prioritize the top human risks in your organization.
• Lab 3: Identify and document the top behaviors (learning objectives) that manage those risks.
• Lab 4: Leverage the AIDA marketing model to engage and communicate to your workforce about a new tool roll-out.
• Lab 5: Create a strategic engagement plan on how you will effectively communicate to and engage your workforce to manage a specific human risk

Additional Free Resources

• Security Awareness Roadmap: Managing Your Human Risk, poster
• 2022 Security Awareness Report™: Managing Human Risk
• Career Development for Security Awareness, Engagement, and Culture Professionals (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.
• Managing Human Risk Should be a Regular Element on Any Cybersecurity Team Guest blog post by Mari Svestad

This Course Will Prepare You to:

• Understand the Security Awareness Maturity Model and how to leverage it as the roadmap for your awareness program
• 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
• Measure the impact of your awareness program, track reduction in human risk, and communicate the program’s value to leadership

“This is an absolutely fantastic course. Lance is a great presenter and held my interest through the entire course. The material is so valuable, I can’t wait to go back and map out my plans on how I’m going to use it.” —Lesley Swann, Baker Donelson

sans.org/mgt433

• Watch a preview of this course
• Discover how to take this course: Online, In-Person
Prioritizing Human Risk

—Lance Spitzner

effectively manages and measures human risk.

the skills, resources, and community they need to build a mature security awareness program that

more resilient organization. I am extremely excited about MGT433, as it provides organizations with

asset, not only to prevent incidents but also to quickly identify and report them, resulting in a far

properly invest in people and secure them. Once trained, your workforce will become your greatest

constant factor: people are the number one attack vector for cyber attackers because we fail to

Having been actively involved in information security for more than 20 years, I have seen one

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 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 security 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

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
• 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

SANS Security Awareness Professional

Organizations seek proven leaders who have the expertise and skills to effectively manage and measure human risk. The SANS Security Awareness Professional (SSAP) provides not only this expertise, but also signifies, documents and certifies that the holder has met the requirements to elevate the overall security behavior of the workforce.

The first step to achieving your SSAP is taking the two-day SANS MGT433 course on building mature awareness programs.

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

— Chris Sorensen, GE Capital