LDR433: **Managing Human Risk™**

SSAP
Secururity Awareness Professional
giac.org/ssap

3 Day Course	18 CPEs	Laptop Not Needed

This Course Will Prepare You to:

- Master how to map and benchmark your program's maturity against your peers'
- Understand the Security Awareness Maturity Model and how to leverage it as the roadmap for your program
- Ensure compliance with key standards and regulations
- Implement models for learning theory, behavioral change, and cultural analysis
- 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
- Explain the most effective ways to communicate to and engage people
- Identify high-risk roles and the required, specialized training for those roles
- Define what security culture is and the common indicators of a strong security culture
- Explain your organization's overall culture and how to most effectively align cybersecurity with and embed security into your organization's culture
- Measure the impact of your program, track reduction in human risk, and how to communicate to senior leadership the value of the program in strategic terms
- Define steps to grow your career, increase your credibility and expand your work options

"I think the course is really engaging and works at two levels: (1) It would provide someone starting out with a solid foundational knowledge, (2) It allows an existing program to benchmark and get new ideas, to supplement the existing work."

—Brian Wright,
Student Loans Company Unlimited

People have become the primary attack vector. Manage your human risk.

Learn the key lessons and the roadmap to build a mature awareness program that will truly engage your workforce, change their behavior and ultimately manage your human risk. Apply models such as the BJ Fogg Behavior Model, AIDA Marketing funnel, and Golden Circle, and learn about the Elephant vs. the Rider. Concepts include how to assess and prioritize your top human risks and the behaviors that manage those risks, how to engage, train and secure your workforce by changing their behaviors and culture, and how to measure the impact and value of that change.

The course content is based on not only learning theory and behavior change models but lessons learned from hundreds of programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers. Finally, you will have the opportunity to earn the SANS Security Awareness Professional (SSAP), the industry standard in human risk management.

What Is Human Risk Management?

Cyber threat actors have changed their attack methods, they no longer target technology but people. Human Risk Management is the structured approach in how organization's secure people, addressing for most organizations what is now their greatest vulnerability—their workforce.

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'soverall risk management efforts
- Make the most of your investment by sustaining your program long term, going beyond changing behavior to embedding a strong security culture
- Communicate and demonstrate the value of the change to your senior leadership in business terms

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 three-section course has eight interactive labs. Each lab is approximately 30 minutes to complete as a team, with another 20–30 minutes of group discussion.

- **Section 1:** Determine Your Program's Maturity Level, Partnering with Others, Tulip Manufacturing: A Risk Case Study
- **Section 2:** Identify and Prioritize the Key Behaviors that Manage Risks, Leverage the AIDA Model to Sell MFA
- **Section 3:** Defining Your Organization's Culture, Creating an Action Plan for When You Return

Additional Free Resources

- Security Awareness Roadmap: Managing Your Human Risk, poster
- Annual Security Awareness Report™: Managing Human Risk
- For those 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.

Section Descriptions

SECTION 1: Fundamentals and Identifying/Prioritizing Human Risk

Section 1 covers the fundamentals by specifically answering what is human risk and how organizations can effectively manage it. We start with students defining the maturity of their existing program and provide a roadmap on how to improve their program maturity. We then cover critical foundations for a successful program; leadership support, a program charter, and an advisory board. We then cover the fundamentals of risk management and how that applies to managing human risk, to include models of behavior change. We finish the day with a process on how to identify and prioritize your top human risks.

TOPICS:

- How to map and benchmark your programs maturity
- The five stages of the Security Awareness Maturity Model
- The fundamentals of risk and risk management
- 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, the behaviors to manage those risks, and 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)
- How to identify and manage role-based risks

SECTION 2: Identifying and Changing Behavior

The second section begins with Artificial Intelligence and how to leverage it to exponentially increase the impact of your program. We then cover how to identify the key behaviors that manage your top human risks, to include defining each behavior as a learning objective. We then cover how to change behaviors at an organizational level, starting with the fundamentals of engagement and motivating change, then how to adapt your program to different demographics, cultures and regions. Finally we go into the many different methods and modalities to train and engage your workforce.

TOPICS:

- Resources for your long-term success
- Latest in Artificial Intelligence/Gen AI and how to leverage it to accelerate your program and career
- Defining learning objectives and how they apply to learning theory and risk management
- How to identify and prioritize the top behaviors that manage your key human risks
- Fundamentals of engaging and changing human behavior
- Introduction of the Golden Circle and the importance of "why"
- How you can effectively create an engagement strategy leveraging marketing models
- Creating a training strategy leveraging the ADDIE and Kirkpatrick models
- 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), virtual live training (VLT) and computer-based training (CBT)
- Different reinforcement methods, including newsletters, infographics, podcasts, micro-videos and video shorts, memes, hosted speaker events, hacking demos, scavenger hunts, virtual lunch-and-learns, and numerous other training activities
- How to put this all together for a specific training/risk management goal

SECTION 3: Security Culture and Measuring Change

This section begins with culture, specifically defining your organization's overall culture, what security culture is and how to embed a strong security culture into your organization's overall culture. We then cover metrics, starting with why we want metrics and how to use them at a strategic level. We then do a deep dive into how to measure behavior and culture, then strategic metrics and then finally how to communicate the value of your program to leadership in business terms. We finish the class with how to put this all together into an actionable plan with key tips for success.

TOPICS:

- We start the day with career development, a series of steps you can take to grow your credibility, position and compensation
- What organizational culture is and how to define your organization's overall culture
- We explain what security culture is, the value of a strong security culture and the most common indicators of both a weak and strong security culture
- How to align with and embed a strong security culture into your organization's overall culture
- How to create a strong incentive program to sustain behavior change long-term
- A deep dive into Ambassador Programs
- Fundamentals of metrics, including why we collect them and how to leverage them strategically
- The difference between compliance metrics and impact metrics
- Walk through of the three types of impact metrics: knowledge, culture and behavior
- What are your leadership's strategic priorities and how to align your strategic metrics framework with those strategic priorities
- Putting an overall project plan together and executing it
- Resources for success moving forward

Who Should Attend

- Security awareness, training, engagement or culture officers
- Security management officials
- Security ambassadors or champions officers
- 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, influence or communications program

NICE Framework Work Roles

- Cyber Instructional Curriculum Developer (OPM 711)
- Security Awareness & Communications Manager (OP 712)

SSAP
Secururity Awareness Professional
giac.org/ssap

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 three-day SANS LDR433 course on building mature awareness programs.