SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

LDR521: **Security Culture for Leaders™**

5 Day Course	30 CPEs	Laptop Required

You Will Be Able To

- Define, map, and measure both organizational and security culture
- Build a practical strategy leveraging the four key drivers of your security culture
- Communicate the business value of security to gain executive buy-in
- Engage and motivate your workforce to prioritize and adopt secure behaviors
- Architect and embed security so it aligns with how people think and operate
- Improve the success of security initiatives with actionable strategies and tools

> **"This content is helping bring back concepts that get forgotten when you go from a doer to a senior leadership role. It brought back good concepts and a way to utilize them in the security context as well as getting leadership to think differently."**
>
> —Michael Neuman

What is a Security Culture?

Security culture is your organization's shared attitudes, perceptions, and beliefs about cybersecurity. The more strongly your leadership and workforce believe in and buy into cybersecurity, the more likely they will prioritize security, support your initiatives, and exhibit the behaviors you want. Your organization already has a security culture. The question is, is it the culture you want?

Build and Measure a Strong Security Culture

Drawing on real-world lessons from around the world, the SANS LDR521 Security Culture for Leaders course will teach you how to build a culture where both your leadership and workforce believe in and prioritize cybersecurity. Through hands-on instruction and a series of interactive team labs and exercises, you will apply organizational change concepts to various real-world security initiatives and quickly learn how to transform your security team and embed security into your organization's culture, from senior leadership on down. Apply findings from Daniel Kahneman's Nobel prize-winning research, Thayler and Sunstein's Nudge Theory, ADKAR change model and Simon Sinek's Golden Circle. Learn how Spock, Homer Simpson, the Elephant and Rider, and the Curse of Knowledge are all keys to building a strong security culture at your organization.

Business Takeaways

- Build a strong, positive brand for you and your security team, be perceived as enablers
- Embed security at the start of all business initiatives
- Increase buy-in and success rates of all security programs
- Gain critical executive leadership support, speak in their language
- Create a workforce that naturally prioritizes security
- Reduce security-team burnout through cultural alignment

Hands-On Security Culture Training

The SANS LDR521: Security Culture for Leaders course empowers cybersecurity leaders with the tools to build, measure, and institutionalize a strong cybersecurity culture across their organization. Through hands-on labs, real-world scenarios, and proven behavioral science frameworks, participants learn how to gain executive buy-in, engage the workforce, and integrate security into everyday business practices. This course is designed for experienced security professionals looking to drive meaningful cultural change and elevate the impact of their security programs.

Notice to Students

The course is recommended for more senior and/or more experienced cybersecurity leaders, managers, officers, and awareness professionals. If you are new to cybersecurity, we recommend some of SANS's more fundamental courses, such as **SEC301: Introduction to Cyber Security**; **SEC401: Security Essentials: Network, Endpoint, and Cloud**; or **LDR433: Human Risk Management**.

sans.org/LDR521

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Fundamentals of Organizational and Security Culture

Learn the fundamentals of culture and how to decipher your organizational and security culture.

TOPICS: Role of Strategy vs. Culture; Defining and Mapping Organizational Culture; Role of AI in Changing Culture; Defining and Indicators of Security Culture; Security Culture Assessment

SECTION 2: Defining Your Strategy

Define what you want your security culture to be and develop an actionable strategy on how to achieve it.

TOPICS: Building Your Strategy to Culture Change; Proven Organizational Change Models and Frameworks; Motivating and Enabling Change; Four Drivers to Your Security Culture; Developing Your Security Principles and Guidelines

SECTION 3: Motivating Change

Section 3 focuses on interpreting vulnerability data, prioritizing in context, and communicating with executives and stakeholders. Labs include contextual prioritization, executive translation, and board briefings. Cyber42 Round 3 is included.

TOPICS: Safety and Motivation Principles; Leveraging Marketing Models and Frameworks; Creating Engagement Personas; Incentivizing Security Behaviors

SECTION 4: Engaging Change

In Section 4, you will learn how to overcome the "Curse of Knowledge" and make security simple for your entire workforce. Master proven models so your security initiatives and priorities align with and become embedded in people's daily processes and activities.

TOPICS: Architecting Security so it Aligns with People's Daily Activities; Address Cognitive Biases Effectively; Building Security Knowledge; Simplifying and Embedding Security Processes

SECTION 5: Measuring Change and Final Steps

In the final section, you will learn how to quantify your security culture and how the changes you are making support leadership's strategic priorities. Sell your security initiatives and priorities in business terms that resonate with leadership.

TOPICS: Design Effective Security Culture Surveys; Analyze and Quantify Metrics for Action Items; Align Metrics with Leadership's Priorities; Build Strong Business Cases; Create Executive-Ready Summaries

> **"Excellent job, Russel! I really enjoyed your technique, caring, thoughtfulness and good vibes you brought to this class."**
>
> —Christopher Jones, **Trinchero Family Estates**

> **"Many ah-ha moments. This material is rich and full of useful tidbits."**
>
> —Kyle Swenson, **Medtronic**

Who Should Attend

- Chief information security officers
- Chief risk officers/Risk management leaders
- Security awareness, engagement or culture managers
- Senior security managers who lead large-scale security initiatives
- Information security managers, officers, and directors
- Information security architects and consultants
- Aspiring information security leaders
- Business continuity/Disaster recover leaders
- Privacy/Ethics officers

NICE Framework Work Roles

- Cyber Instructional Curriculum Developer (OPM 711)
- Security Awareness and Communications Manager (OPM 712)
- Information Systems Security Manager (OPM 722)
- Cyber Workforce Developer and Manager (OPM 751)
- Cyber Policy and Strategy Planner (OPM 752)
- Executive Cyber Leadership (OPM 901)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)

Course Author Statement

"For far too long, security teams have struggled with the human side of cybersecurity. Security culture is not nearly as hard as many believe; you have to approach the challenge differently than most people are used to; instead of fighting human nature, this course is all about aligning with human nature. LDR521 arms you with the knowledge, skills, and resources to institutionalize a strong security culture so your organization believes in and prioritizes cybersecurity. In addition, the course will provide you the resources to measure and communicate the impact to members of your leadership, ensuring their long-term support."

—Lance Spitzner