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

GIAC CERTIFICATIONS

LDR521: **Security Culture for Leaders**

5	30	Laptop
Day Course	CPEs	Required

You Will Be Able To

- Explain what culture is, its importance to security, and how to map and measure both your organization's overall culture and your security culture.
- Define the indicators of a strong security culture, align security with them, and embed them into your organization's existing culture.
- Provide a framework and guiding principles for your security team on how to lay the foundation for a strong security culture.
- Effectively communicate the business value of security to your Board of Directors and executives, gaining their support and buy-in.
- Engage and motivate your workforce so they prioritize cybersecurity.
- Simplify security and remove blockers, making it exponentially easier for people to embed security into their everyday actions.
- Dramatically improve the effectiveness and impact of your security initiatives, such as DevSecOps, cloud migration, vulnerability management, Security Operations Center, incident detection and response, and other related security projects.
- Measure your security culture, how to make those measurements actionable, and how to present the maturity and value of your security culture to leadership
- Leverage numerous templates and resources from the Digital Download Package and Community Forum that are part of the course and which you can then build on immediately.

> **"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 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

- **Security at Scale—**Make your job easier by scaling both yourself and your security team. Reduce the impact of burnout on the security team you are privileged to lead.
- **Embed Security—**Automatically bake security into the start of every business project and initiative in every business unit of your organization.
- **Executive Support—**Get the executive leadership support you need for what is most important to you.
- **Secure your Workforce—**People will exhibit the behaviors you want without telling them what they can and cannot do at work.
- **Successful Initiatives—**Make your security initiatives far more successful by gaining the buy-in of key departments, such as IT, Engineering, and the Business.
- **Advocates—**Transform your security team into security advocates who engage, motivate, and enable your workforce to be far more secure.

Hands-On Security Culture Training

The first four sections of the course leverage 11 interactive team labs, enabling you to apply the lessons learned to a variety of real-world security situations and challenges. These team labs enable you to learn from the instructor and course materials and your fellow students' expertise and experiences. Finally, the last section is a capstone event as you work through a series of case studies to see which team can create the strongest security culture. Leveraging the Cyber42 simulation game environment, you are put in real-world scenarios that spur discussion and critical thinking of situations you will encounter at work as you compete for the LDR521 Challenge coin. A Laptop with access to the internet is required for the Cyber 42 leadership simulation capstone.

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: Managing Human Risk or LDR419: Performing A Cybersecurity Risk Assessment.

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

Section 1 begins by demonstrating how security is no longer just about technology but also about people and culture. We then explain what culture is, why it is so important, and how it applies to security. We then demonstrate how to identify and map your organization's overall culture, identify your organization's current security culture, and then determine the security culture you want to achieve. We will then cover several models and the best approach on how to achieve your desired security culture.

TOPICS: Human Side of Security; Case Study – Microsoft Cybersafety Review Board Report; Defining Culture; Mapping Organizational Culture; Defining and Mapping Security Culture; Identifying Desired Security Culture; Organizational Change Frameworks; Motivating and Enabling Change

SECTION 2: Motivating Security Culture

Section 2 focuses on motivating people and explaining the "why" of security. Far too often, security fails because security teams mandate what people must do and punish those who fail to follow policy or exhibit the desired behaviors. As a result, there is a great deal of resistance from the workforce. In this section, we'll walk you through how to engage and motivate your workforce effectively so they believe in and prioritize cybersecurity, including leveraging marketing models, implementing incentive programs, and targeting specific and global audiences.

TOPICS: SLeveraging AI in Building Security Cultures; Safety: Survive vs. Thrive; Start With Why; Know Your Audience; Marketing Change; Motivating Global Change; Incentivizing Change

SECTION 3: Enabling and Measuring Security Culture

Section 3 begins with one of the most common reasons organizations have a toxic security culture—security is too hard. People want to do the right thing but don't know where to start. We have to enable people, so security is simple for them. This begins with the concept of the Curse of Knowledge: the more of an expert you are at security, the more likely you don't realize just how confusing and difficult security is for others. We address this by first imparting knowledge—training people and providing them with the skills to be successful. We then simplify what is expected of them by making security as easy as possible. Far too often, the policies, processes, and communications we create are complex, intimidating, or difficult to follow. Finally, we'll cover how to track, measure, and communicate the impact of your security culture.

TOPICS: Cognitive Biases; Building Knowledge; Simplifying Security; Measuring Change

SECTION 4: Engaging Leadership

Up to this point, we have covered creating a strong security culture within your workforce. This section covers how to do the same thing but with your executive leadership. A strong security culture depends on the support of your executives, but to get their support, you have to speak their language. This section covers the key elements and frameworks for creating a high-impact business case, including a dive into the financial statements of several organizations.

TOPICS: Building Your Business Case; Financing Your Business Case; Communicating Your Business Case; What Will This Make Possible?

SECTION 5: Capstone Workshop

In the final section, you will combine and apply everything you have learned through a series of interactive team labs. Your mission is to work as a team to make tough decisions as you create a strong security culture at the fictional company, Linden Insurance. Each of the labs builds on the previous labs, with the decisions you make in each lab impacting not only your score but what decisions you can make in future labs—just like in real life! For the capstone, you will leverage the Cyber42 simulation game environment, spurring discussion and critical thinking about situations you will encounter at work. Each member of the winning team will take home the highly coveted LDR5 21 Challenge Coin!

"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 and Russell Eubanks