LDR521: **Security Culture for Leaders**

5 Day Course	30 CPEs	Laptop Required

You Will Be Able To

- Explain what organizational culture is, its importance to security, and how to map and measure both your organization's overall culture and security culture
- Align your security culture to your organization's strategy, including how to leverage different security frameworks and maturity models
- Effectively communicate the business value of security to your Board of Directors and executives and more effectively engage and motivate your workforce
- Enable and secure your workforce by integrating security into all aspects of your organization's culture
- Dramatically improve both 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
- Create and effectively communicate business cases to leadership and gain their support for your security initiatives
- Ability to 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

"I am just so happy with this material focusing on embedding secure values into our global culture – exactly what my company needs help with NOW."

—Lindsay O'Bannon, **Deloitte Global**

What is a Security Culture?

Security culture is your workforce's shared attitudes, perceptions, and beliefs about cybersecurity. It is what they think and feel about your security team, your security policies, and your security training. The more positive their attitudes towards your security team, the more they will trust your security team. The higher their perception that your security team is committed to your company's mission, the more likely they will exhibit more secure behaviors. The greater their belief in your security training, the more likely they will commit to your organization's security culture.

Build and Measure a Strong Security Culture

Drawing on real-world lessons from around the world, the SANS LDR521 security culture for leadership course will teach you how to leverage the principles of organizational change to develop, maintain, and measure a strong security culture. Through hands-on instruction and a series of interactive labs and exercises, you will apply these concepts to various real-world security initiatives and quickly learn how to 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, 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 company.

Business Takeaways

- Create a far more engaged and secure workforce, not only in their attitudes about security but also in their behaviors
- Dramatically improve the ROI of security initiatives and projects through increased success and impact
- Strengthen communication between the security team and business executives
- Instill stronger and more positive attitudes, perceptions, and beliefs about the security team
- Construct simpler, more effective security policies and governance

Hands-On Security Culture Training

The first four sections of the course leverage 12 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 not only from the instructor and course materials but also from 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 that you will encounter at work. A Laptop 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.

Section Descriptions

SECTION 1: Fundamentals of Culture and Organizational Change

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, than 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 – Equifax Congressional Report; Defining Culture; Mapping Organizational Culture; Defining and Mapping Security Culture; Identifying Desired Security Culture; Change Management Frameworks; Motivating and Enabling Change

SECTION 2: Motivating Change

Section 2 focuses on motivating people and explaining the "why" of security. Far too often, security fails because security teams simply mandate what people must do and then 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 effectively engage and motivate your workforce, including leveraging marketing models, implementing incentive programs, and targeting both specific and global audiences. As a result security and the security team are perceived as helpful, collaborative and enablers, your first step to building a strong security culture.

TOPICS: Safety: Survive vs. Thrive; Start With Why; Know Your Audience; Marketing Change; Motivating Global Change; Incentivizing Change

SECTION 3: Enabling and Measuring Change

Section 3 begins with the concept of 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. One of the most common reasons organizations have a toxic security culture is security overwhelms people. We have to enable people so security is simple for them. This begins with imparting knowledge - that is, 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 procedures 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: Making the Business Case

Up to this point we have covered how to create a strong security culture within your workforce. In this section we cover 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. In this section we cover the key elements and frameworks for putting together a high-impact business case, including a dive into financials.

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 teams to make some very tough decisions as you create a strong security culture at Linden Insurance. Each of the labs build 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 of situations that you will encounter at work.

"Excellent job, Russel! I really enjoyed your technique, caring, thoughtfulness and good vibes you brought to this class."

—Christopher Jones, **Trinchero Family Estates**

"Lance was fantastic! He made the course super engaging and covered all information thoroughly, making sure to draw in and leverage student experience to make the course richer."

—Anna Troutman

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, cybersecurity has been perceived as purely a technical challenge. Organizations and leaders are now realizing that we also have to address the human side of cybersecurity management. From securing your workforce's behavior to engaging and training developers, IT staff, and other departments, security today depends on your ability to engage and partner with others. In other words, your security culture is becoming just as important as your technology. LDR521 will provide the frameworks, roadmaps, and skills you need to successfully embed a comprehensive, organization-wide cybersecurity culture. 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