MGT521: Leading Cybersecurity Change: Building a Security-Based Culture

5	30	Laptop
Day Course	CPEs	Not Needed

You Will Be Able To

- More effectively communicate the business value of cybersecurity to your Board of Directors and executives, improve collaborate with your peers, and more effectively engage your workforce
- Explain what organizational culture is, its importance to cybersecurity, and how to map and measure both your organization's overall culture and security culture
- Align your cybersecurity culture to your organization's strategy, including how to leverage different security frameworks and maturity models
- Explain what organizational change is, identify different models for creating change, and learn how to apply those models
- Enable and secure your workforce by integrating cybersecurity 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 and other related security deployments
- Create and effectively communicate business cases to leadership and gain their support for your security initiatives
- How to measure your security culture and how to present the impact of a strong 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 right away

Build and Measure a Strong Security Culture

Drawing on real-world lessons from around the world, the SANS MGT521 course will teach you how to leverage the principles of organizational change in order to develop, maintain, and measure a security-driven culture. Through hands-on instruction and a series of interactive labs and exercises, you will apply these concepts to a variety of different real-world security initiatives and quickly learn how to embed cybersecurity into your organization's culture immediately.

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 all are keys to building a strong cybersecurity culture at your company.

Business Takeaways

- Create a far more secure workforce, both in their attitudes about cybersecurity and also in employee behaviors
- Enable the security team to create far stronger partnerships with departments and regions throughout the organization
- Dramatically improve the ROI of cybersecurity initiatives and projects through increased success and impact
- Improve communication between the cybersecurity team and business leaders
- Create stronger and more positive attitudes, perceptions and beliefs about the cybersecurity team

Hands-On Training

This five-section course includes 16 interactive labs that walk you through exercises and apply the lessons learned to a variety of typical real-world security situations and challenges. Many of the labs are carried out as teams, ensuring that you learn not only from the course materials but from other students and their 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. Culture is a very human and global challenge, and as such we want to expose you to as many different situations and perspectives as possible.

Notice to Students

The course is recommended for more senior and/or more experienced cybersecurity managers, officers, and awareness professionals. If you are new to cybersecurity, we recommend some of SANS's more basic courses, such as SEC301, SEC401, or MGT433.

"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**

sans.org/mgt521

- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Fundamentals of Culture and Organizational Change

Section 1 begins by demonstrating how cybersecurity is no longer just about technology but also about culture. We explain what organizational culture is, why it is so important and how it applies to cybersecurity. We then demonstrate how to 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 organizational change and on how to achieve your desired, strong 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; Defining and Leveraging Change Management Frameworks; Project Charters

SECTION 3: Enabling and Measuring Change

Section 3 begins with enabling and the concept of Curse of Knowledge. Communicating to and engaging is only half the battle. We also 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 change.

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

SECTION 5: Capstone Workshop

In this final course 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 attempt to create a strong security culture at Linden Insurance. The decisions you and your team make in each lab will impact your team's Culture Score. Each of the five 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!

SECTION 2: Motivating Change

Section 2 focuses on motivating people and explaining the "why" of cybersecurity. Far too often, security fails because security teams simply mandate what people must do and how to do it but never explains why. As a result, there is a great deal of resistance to attempts to change workforce behavior and implement security initiatives such as DevSecOps or vulnerability management. In this section, we'll walk you through the key elements of explaining why change is needed, including leveraging marketing models, implementing incentive programs, and targeting both specific and global audiences.

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

SECTION 4: Making the Business Case

Up to this point we have covered how to communicate to, engage and motivate your workforce. In this section we cover how to do the same thing but with your business leadership. A strong cybersecurity 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?

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

Who Should Attend

- Chief information security officers
- Chief risk officers/Risk management leaders
- Security awareness/Engagement 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

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. MGT521 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

> **"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