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 to your Board of Directors and executives, collaborate with your peers, and engage your workforce
- Explain what 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 large-scale security initiatives
- Create and effectively communicate business cases to leadership and gain their support for your security initiatives and security in general
- 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

Cybersecurity management is no longer just about technology. It is ultimately about organizational change - change not only in how people think about security but in what they prioritize and how they act, from the Board of Directors to every corner of the organization. Organizational change is a field of management study that enables leaders to analyze, plan, and then improve their operations and structures by focusing on people and 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 the concepts of organizational change to a variety of different security initiatives and quickly learn how to embed security into your organization's culture.

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.

Lab Information

This five-session course includes 17 interactive labs that walk you through exercises and apply the lessons learned to a variety of typical real-world 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. 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. **No Laptop Required. "Labs" are group case studies with no computers needed.**

What You Will Receive

- Digital Download Package: A collection of templates, checklists, matrices, reports, and other resources that will help you in your cybersecurity career. This package is continually updated and is based on resources that real cybersecurity leaders have used in developing their own cybersecurity cultures. Why reinvent the wheel when you can reuse or reshape what has worked for others!
- Community Forum: An opportunity to join the private, invitation-only Community Forum dedicated to the human element. The forum currently has over 1,500 active members!

Section Descriptions

SECTION 1: Fundamentals of Organizational Change

Section 1 begins by demonstrating how cybersecurity management is ultimately about organizational change. Technology alone will no longer solve security problems. We explain what culture is and how it applies to cybersecurity, how to map your organization's overall culture, and then determine the security culture you want and how to align it with your organization's culture. We will then cover organizational change and different models for changing an organizational 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 2: Motivating Change

Section 2 focuses on motivating people and explaining the "why" in change. Far too often, security fails because it dictates 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 3: Enabling and Measuring Change

Communicating with people and engaging and motivating them is only half the battle. We also have to enable people to change. 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 4: Making the Business Case

Up to this point we have covered how to communicate with your workforce and engage and motivate various departments. In this section we cover how to do the same thing 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

SECTION 5: Capstone Workshop

In this final course section you will combine and apply everything you have learned through a series of labs. Your mission is to work as teams to make some very tough decisions as you attempt to secure Linden Insurance during a crisis. The decisions you and your team make in each lab will impact your team's Culture Score. Each of the six 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!

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