LDR514: Security Strategic Planning, Policy, and Leadership

GSTRT
Strategic Planning, Policy & Leadership
giac.org/gstrt

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Develop strategic security plans
- Create effective information security policy
- Understand the different phases of the strategic planning process
- Increase your knowledge of key planning tools
- Cultivate fundamental skills to create strategic plans that protect your company
- Enable key innovations
- Facilitate working effectively with your business partners
- Advance security strategic plans that incorporate business and organizational drivers
- Foster and assess information security policy
- Use management and leadership techniques to motivate and inspire your team

Business Takeaways

- Create a security plan that resonates with customers
- Develop leaders that know how to align cybersecurity with business objectives
- Build higher performing security teams

"I enjoy the use of Cyber 42. I particularly enjoyed the extra addition of going through the answers and discussing which answers had what effects to everyone's scores."

—Alexander Walker, **TechVets**

"I love the lab and exercises. They are exactly what I am looking for as the new Marketplace Security PM on my team."

—Rebecca Gaudet, **Microsoft**

Aligning Security Initiatives with Strategy

As security professionals, we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny. This course gives you tools to become a security business leader who can build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams.

Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. These policies must be aligned with an organization's culture. In LDR514, we break down the steps to policy development so that you have the ability to design and assess policies that can successfully guide your organization.

Leadership is a skill that must be learned, exercised, and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and having the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives, removing the obstacles preventing them from doing it, and maintaining the well-being of the team in support of the organization's mission. LDR514 will teach you to use management tools and frameworks to better lead, inspire, and motivate your teams.

What Is Cyber Security Strategy?

Simply put, strategy is the ability to get from one place to another in a beneficial way. Your job as a leader is to figure out how to do that for your business, your team, and yourself. You need a wide combination of skills that go beyond the technical nitty gritty to progress into a more senior leadership role and build rapport with executive leadership. This includes being able to build a strategic plan, conduct gap analysis, understand both the business and threat landscape, build a compelling business case, and create effective security policy. On top of all this you must ensure that your team can actually get the work done by leading, motivating, and inspiring them to actually WANT to get the work done. In summary, the ability to build a cybersecurity strategy will help you take the next step in your career, build higher performing teams, and align cybersecurity with business objectives.

Hands-On Training

LDR514 uses business case studies, fictional companies, and the Cyber42 leadership simulation game to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. This web application-based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

The course also uses case studies from Harvard Business School, case scenarios, team-based exercises, and discussions that put students in real-world situations. You will be able to use these same activities with your own team members at work.

Section Descriptions

SECTION 1: Strategic Planning Foundations

Creating security strategic plans requires a fundamental understanding of the business and a deep understanding of the threat landscape. Deciphering the history of the business ensures that the work of the security team is placed in the appropriate context. Stakeholders must be identified and appropriately engaged within this framework. This includes understanding their motivations and goals, which is often informed by the values and culture your organization espouses. Successful security leaders also need a deep understanding of business goals and strategy. This business understanding needs to be coupled with knowledge of the threat landscape—including threat actors, business threats, and attacker tactics, techniques, and procedures—that informs the strategic plan.

TOPICS: Strategic Planning Overview; Decipher the Business; Decipher the Threats

SECTION 2: Strategic Roadmap Development

With a firm understanding of the drivers of business and the threats facing the organization, you will develop a plan to analyze the current situation, identify the target state, perform gap analysis, and develop a prioritized roadmap. In other words, you will be able to determine (1) what you do today (2) what you should be doing in the future (3) what you don't want to do, and (4) what you should do first. Once this plan is in place, you will learn how to build and execute it by developing a business case, defining metrics for success, and effectively marketing your security program.

TOPICS: Define the Current State; Develop the Plan; Deliver the Program

SECTION 3: Security Policy Development and Assessment

Policy is one of the key tools that security leaders have to influence and guide the organization. Security managers must understand how to review, write, assess, and support security policy and procedures. This includes knowing the role of policy in protecting the organization along with its data, systems, and people. In developing policy, you also need to know how to choose the appropriate language and structure so that it fits with your organization's culture. As policy is developed you must manage the entire lifecycle from approval and socialization to measurement in order to make necessary modifications as time goes on. This is why assessing policy and procedure is so important. Policy must keep up to date with the changing business and threat landscape. This includes coverage of technologies like Generative Artificial Intelligence (GenAI).

TOPICS: Purpose of Policy; Develop Policy; Managing Policy; Assess Policy and Procedure

SECTION 4: Leadership and Management Competencies

This course section will teach the critical skills you need to lead, motivate, and inspire your teams to achieve your organization's goals. By establishing a minimum standard for the knowledge, skills, and abilities required to develop leadership, you will understand how to motivate employees and develop from a manager into a leader.

TOPICS: Why Choose Leadership; Leadership Essentials; Effective Communication; Build Effective Teams; Leading Change

SECTION 5: Strategic-Planning Workshop

Using case studies, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. The case studies are taken directly from Harvard Business School, which pioneered the case study method. The case studies focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, enabling students to synthesize and apply concepts, management tools, and methodologies learned in class.

TOPICS: Creating a Presentation for the CEO; Briefing the Board of Directors; Creating a Strategic Plan; Understanding Business Priorities; Enabling Business Innovation; Effective Communication; Stakeholder Management

"[The] strength of the course is live labs and exercises."

—Ajay Kumar, **National Grid**

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Security personnel who have team lead or management responsibilities
- Anyone who wants to go beyond technical skills
- Technical professionals who want to learn to communicate with senior leaders in business terms

NICE Framework Work Roles

- Executive Cyber Leadership (OV-EXL-001)
- Information Systems Security Manager (OV-MGT-001)
- Program Manager (OV-PMA-001)
- IT Project Manager (OV-PMA-002)
- Cyber Workforce Developer and Manager (OV-SSP-0001)
- Cyber Policy and Strategy Planner (OV:-SPP-002)

GSTRT
Strategic Planning, Policy & Leadership
giac.org/gstrt

GIAC Strategic Planning, Policy, and Leadership

The GIAC Strategic Planning, Policy, and Leadership (GSTRT) certification validates a practitioner's understanding of developing and maintaining cyber security programs as well as proven business analysis, strategic planning, and management tools. GSTRT certification holders have demonstrated their knowledge of building and managing cyber security programs with an eye towards meeting the needs of the business, board members, and executives.

- Business and Threat Analysis
- Security Programs and Security Policy
- Effective Leadership and Communications