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

- Build cybersecurity strategic plans aligned with business objectives
- Develop and assess effective information security policies
- Apply business and risk analysis techniques to security initiatives
- Communicate security priorities clearly to executives and boards
- Lead and motivate high-performing cybersecurity teams

Business Takeaways

- A defensible security strategy aligned to organizational goals
- Stronger executive and board support for security initiatives
- Improved risk management through clear policy and governance
- More effective allocation of security resources and investments
- Measurable security outcomes tied to business performance

> **"I enjoyed 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**

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 Cybersecurity 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-based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at the fictional organizations in the course. 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

Section 1 presents strategic planning tools to decipher the business and the threat landscape. This section examines stakeholder identification and ways to gain executive support through exercises including asset analysis, stakeholder management, and strategy maps, students practice creating plans that resonate with executives.

TOPICS: Strategic Planning Overview; Decipher the Business; Values and Culture; Stakeholder Management, Asset Analysis; Business Strategy; Decipher the Threats; PEST Analysis; Threat Analysis

SECTION 2: Strategic Roadmap Development

Section 2 establishes methodologies for analyzing security posture, identifying target states, and developing prioritized roadmaps. Students learn to assess organizational vision, conduct SWOT analysis, and apply security frameworks. The section covers business case creation and metrics for effectively marketing security initiatives.

TOPICS: Define the Current State; SWOT Analysis; Develop the Plan; Security Framework; Roadmap Development; Business Case Development; Deliver the Program; Marketing Best Practices; Board and Executive Communications

SECTION 3: Security Policy Development and Assessment

Section 3 explores policy as a security leadership tool for guiding organizational behavior. Participants learn methods for developing policies aligned with corporate culture. The section covers policy lifecycle from creation to measurement, with a focus on governance and emerging technology considerations such as Generative Artificial Intelligence (GenAI).

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

SECTION 4: Leadership and Management Competencies

Section 4 addresses critical skills for leading, motivating, and inspiring security teams. Participants develop knowledge and abilities essential for transitioning from management to leadership. The section establishes standards for effective leadership and explores methods for employee motivation aligned with organizational goals.

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

SECTION 5: Strategic-Planning Workshop

Section 5 applies course concepts through Harvard Business School case studies focused on information security leadership. Participants analyze real-world scenarios that reinforce management competencies. The Strategic Planning Workshop serves as a capstone exercise where students synthesize methodologies and tools from previous sections.

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**

> **"This course is a cyber leadership MBA in five days. As a security manager of many years, the class delivered material of great value that I can immediately apply to make a difference at my company."**
>
> —Dave Ferguson, CareFirst

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

- 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)

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