G. Bina
Secure Your Cyber-Space & IT

Executive CISO Seminar

A 3 day learning program which Include demonstrations of the Israeli security management state of the art methodologies

Developed by Dr. Col. (res.) Gabi Siboni

Executive CISO Seminar

A 3 day course

Introduction

As Trends like Cloud based computing, work-from-anywhere and BYOD keep increasing and becoming legitimate and as organizations are facing new government regulations and new compliances The Chief Information Security Officer (CISO) role is developing, changing dramatically and becoming more and more challenging.

Effective security requires a balance of technical and managerial excellence. This program designed to address the relevant knowledge needed by today's cyber leaders and focus on the best practice technologies and tools and it helps technical managers become better security leaders.

About the Course Owner and Developer

This course is developed by Dr. Col. (res.) Gabi Siboni, Director of The Cyber Security Program at The Institute for National Security Studies, Tel Aviv University and Serves as chief methodologist of the IDF's Research Center for Force Utilization and Buildup – Experimentation Laboratory.

Dr. Siboni is a domain expert in national security, military strategy and operations, military technology, cyber security and warfare, and force buildup and a thought leader in business operations risk management.

Who Should Attend?

Information security managers, developers and CIOs who are seeking for a full spectrum and understanding of the Cyber-security domain including operations methodologies, developing cyber workforce and planning and building organization's cyber capabilities.

Course Curriculum

This unique curriculum presents the state of the art Israeli cyber defense and information security methodologies and know-how and demonstrate competency in the design and implementation of a successful cyber-security project.

Topic	Contents
Introduction to the CISO World	The CISO need, the evolution of the CISO, CISO roles and responsibilities CISO Characteristics, CISO challenges
IT and Security Strategic Planning, Policy and Leadership	Mastering the strategic planning process, creating effective information security policy, planning to ensure institutional effectiveness, comprehensive security policy assessment, leadership and management competencies.
Enterprise Security Governance, Compliance and Regulations	Defining corporate IT governance, InfoSec governance, IT & InfoSec governance relationship
Threats, Vulnerabilities	Recognizing technical, behavioral, and organizational threats, mobile and BYOD threats, social media security challenges
Attack and Defense Techniques	Attacks types, Defensive methodologies, trusted computing
Operational and IT Risk Management	Risk management fundamentals, risk assessment, qualitative and quantitative assessment, the hybrid approach, asset management, identifying asset vulnerability, formalizing risk statement, prioritizing risk, stating solutions
Managing Crisis and Resiliency	Developing crisis strategy, Business Impact Analysis (BIA) and Business Continuity Plan (BCP)
Protecting the Organization Critical Infrastructure	Special considerations and resilience, cyber-security and physical-security intersections
SOC and Incident Response	SOC Operation, Incident response methodology, security severity, event categorization and incident escalation
Data Leakage	Data leakage threats, Type of data leakage, mitigation and Data Leakage Prevention (DLP) tools.
Security Investment & Security Measurement	Budget planning Security ROI, security business case, corrective action impact and priority, Project Scoping, Project Investment Control
Intro to digital investigations and Forensics Analysis	Forensic process, digital evidence, investigative tools

* * Learning materials will be provided to participants by a magnetic means