Cyber Security: Information Security Management Best Practice

Date	Venues	($)Fees	Book your seat
14 Dec -18 Dec 2025	Kuala Lumpur	3300	Register Now

Objectives

By the end of the course, participants will be able to:

- Apply information security standards to their organization and its critical assets
- Identify the threats presented by viruses, malware, active code, and Active Persistent Threats (APT)and consider the different mitigating options
- Formulate and manage effective cyber security teams, and apply the Computer Security Incident Response Team (CSIRT) framework, tools and capabilities to deliver cost effective and robust solutions to protect the organization
- Use Neuro Linguistic Programing (NLP) to deliver messages that will change the way employees work and think about security
- Examine the area of wireless security protocols, their security attributes, and their potential in securities within the organization, and in public spaces
- Illustrate how penetration testing and ethical hacking enhance organizational security
- Evaluate and apply two of the most important aspects in the modern day of cyber-adversity: Open Source Intelligence (OSINT) and cyber threat intelligence

Course Outline

Adapting to evolving standards

- Information security standards (e.g. PCI-DSS/ISO27001)
- Documented tools:
- ISO/IEC 27001
- PAS 555
- Control Objectives for Information and Related Technology (COBIT)
- Future standards
- ISO/IEC 2017
- EU privacy regulations
- Local and international government stipulations implicating access to private data

Principles of IT security

- Enterprise security
- External defenses
- Web filtering
- Intruder Prevention Systems(IPS)

- Intruder Detection Systems(IDS)
- Firewalls
- Secure code
- Software Development Life cycles (SDL)
- Potential in securities within developed applications
- WiFi security protocols and attributes
- Voice over IP (VoIP)security
- Governance Risk and Compliance (GRC)
- Security Incident Event Management (SEIM) applications
- Cloud security
- Third party security and compliance

Adopting cyber security measures

- Employee perception on security through Neuro Linguistic Programing (NLP)
- Security education and awareness: techniques, systems, and methodologies
- Penetration testing
- Ethical hacking
- Options to mitigate viruses, malware, active code threats and Active Persistent Threats (APT)
- The Computer Incident Response Team (CSIRT) frameworks, tools and capabilities
- Incident first response:proven methodologies, tools, and systems
- The science of applying robust digital forensics: applicable law, capabilities, and methodologies
- Supervisory Controls and Data Acquisition (SCADA); security requirements, processes and methodologies
- Abuse images: complying with local and international law

Building cyber security teams

- Creation and management of a Secure Operations Center (SOC)
- Development of the Corporate Security Organization Framework
- Formulation and deployment of a Computer Security Incident Response Team (CSIRT)
- Bespoke Security Incident and Event System (SIEM) for the operational deployment
- Risks associated with I/O Security (e.g. USBs, CDs, other forms of media)
- Risks of Active Code Injection, and mitigation techniques

Advanced cyber risks and tools

- Cyber crime and the dark net/dark web: the world of the hackers/hacktivists
- The underground of cyber criminality
- Social engineering as a tool to test operational resilience
- Open Source Intelligence(OSINT)
- Cyber threat intelligence
- Open source and commercial security tools
- The operational use of encryption
- Virtual private networks

WORKSHOP STYLE

A mixture of short presentations, interactive discussion, individual exercises and group work. The emphasis throughout is on a practical approach using case material and examples.

💬 97337256847
✉ info@firstselectbh.com
💻 www.firstselectbh.com