Cybersecurity Training Programme
Module 1

This multi-module training programme is designed to give professionals -at all levels- an in-depth understanding of cybersecurity issues. The programme specifically designed for the Korean market is intended to equip attendees with the latest information and skills to better handle information security in their company.

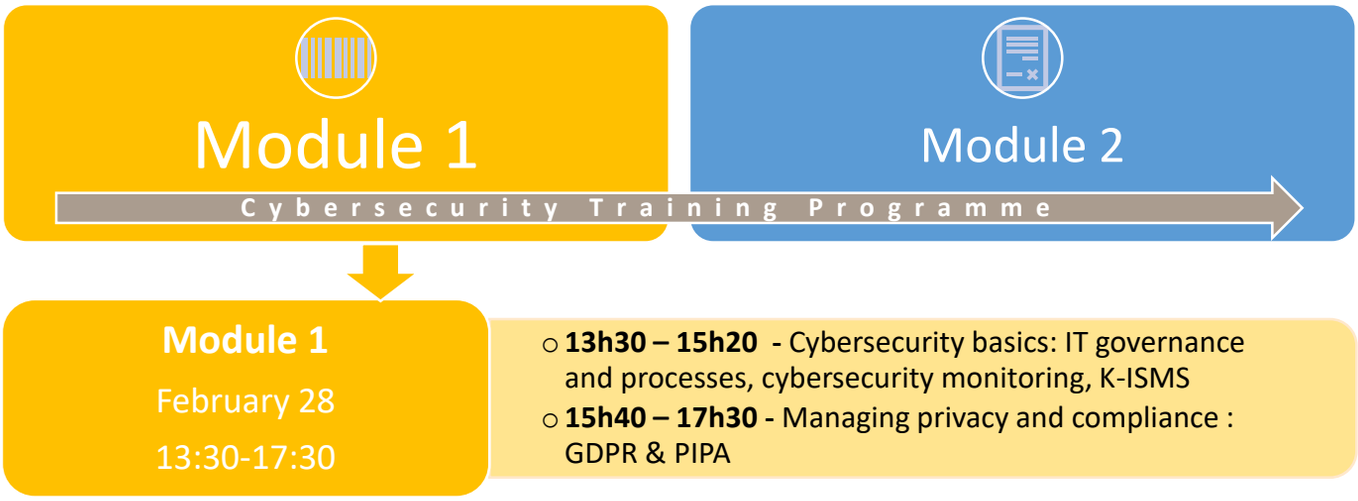
Objectives

- Refresh knowledge on cybersecurity fundamentals
- Provide professional with up-to-date developments of cybersecurity, including specifics of the Korean environment
- Provide the appropriate data protection training to personnel having access to systems
- Equip attendance with latest strategy to identify, contain, address the IT menaces and vulnerabilities
- Zoom on specifics cybersecurity topics: Privacy, compliance, risk management, penetration testing, ethical hacking, cloud security, vulnerability assessment, cryptography, cybersecurity frameworks.

Public

- Non-IT professionals dealing with sensitive corporate Information
- IT professionals

Prerequisite : No prior knowledge of or experience with cybersecurity is necessary



Module 1

February 28

13:30-17:30

- **13h30 – 15h20** - Cybersecurity basics: IT governance and processes, cybersecurity monitoring, K-ISMS
- **15h40 – 17h30** - Managing privacy and compliance : GDPR & PIPA

Topics covered

Cybersecurity Basics

- Cases in Korea
- Managed Cybersecurity Framework
- Risks and Controls, Data Lifecycle
- CISO rôle & KPIs
- Secure Configuration
- Network Security
- Managing User Privileges
- User Education and Awareness
- Incident Management
- Malware Prevention
- Monitoring, Indicators of Compromise
- Cloud Architecture, IOT issues
- Third Party provider management
- Other Risks areas : SDLC, Admin Users Activities, Interface and Error Handling processes

Privacy and Compliance

- Data Privacy Essentials : Data Lifecycle, Privacy, Confidentiality, Personal Information
- Regulation Overview : GDPR & PIPA principles, rules & fines
- DPO basics
- Perimeter Definition and System Analysis
- Data ownership, Data Stewardship
- GDPR compliance initiatives, Setting-up a Privacy Programme
- Data Protection Impact Assesment
- Security Control Design and Implementation
- Policy and Documentation Management
- Communication, Training and Awareness plans
- Data breaches, Incident Management, Monitoring and Evaluation