Cyber Security – An Overview

Course Introduction

The course is designed to give experienced telecoms and computer network professionals additional cybersecurity skills, allowing them to focus on how end to end network protection is optimized.

For Executives without a background in networking who are tasked with protecting their company against cyber-attacks, the course provides an appreciation of network vulnerabilities used by hackers, and the techniques used to thwart them.
Internet users will gain valuable insights on how to keep themselves protected and to prevent exposure to vulnerable network.

Key Benefits

The ever present threat of cyber-attack. Which can paralyse a laptop, a corporation or a government, requires a portfolio of weapons to be maintained in the cyber armoury to protect and deter.

A virus protection programme, a firewall, or network redundancy scheme used in isolation will rarely provide adequate protection.

This course not only gives an overview of the latest protection mechanisms, but describes also how a multifaceted protection solution should be adopted, to keep up with the evolving threat,

Course Objectives

After attending the training, participants will be able to

- Describe the principle types of security threat to which individual computer users, governments, SME's and large corporations are exposed.
- Describe the strengths and weaknesses of defence mechanisms which are deployed by end users, network administrators and network operators to overcome security threats.

- Understand the separate motivations of hackers, crackers and risk managers and the role that each plays in the current cybersecurity landscape.
- Appreciate the evolution of the technology involved in cybersecurity, including concepts such as encryption, firewalls, layering, redundancy, identity and authentication.
- Appreciate the increasing importance of cybersecurity in internet based products, particularly arising from the growth in cloud computing
- Develop a war gaming approach to testing the security of networks

Who should attend?

Network Security Executives, Network Security Auditors, Business Continuity Professionals, Telecom and Computer Network Engineers, Strategic Network Planners, Security Product Development.

Course Duration

2 – day instructor led training event.

COURSE OUTLINE

- What is Cyber Security?
- Terminology
- Types of attack and motivation
- Cyber Crime
- 'Hacktivism'
- Cyber Espionage and Cyber War
- Top target analysis
- The Cost of cyber attacks
- Hacking vs Cracking
- Attack surface and Weak points of entry
- Malware and Viruses
- Denial of Service attacks
- Risk Management
- Cryptography and Encryption
- Passwords
- Identity
- Authentication Legal intercept
- Firewalls

- Deep packet inspection
- Security and products
- Cloud security
- IOT and security
- Security solution cost benefit analysis
- Intrusion detection
- Incident response
- Redundancy
- Confidentiality, Integrity, Availability
- War Gaming
- Cyber Congress (Doha 2015)
- Cyber Attacks – Current Trends
- Cyber Security – Best Practice
- Cyber Security Solutions – A comprehensive strategy
- Case studies