INTRODUCTION TO CYBER SECURITY FOR IT PROFESSIONALS

This course is designed to provide knowledge of information security principles to IT professionals and other associated professions with an IT background including project managers, business continuity professionals, managers and executives.

OUTCOMES

- An understanding of cyber security as a risk to technology, data and business objectives
- The application and relevance of information security principles to the design and operation of secure systems
- An understanding of how the ubiquitous integration of systems aggregates cyber risks
- An appreciation of the current cyber threat landscape
- An awareness of major cyber security controls (access control, cryptography, network filtering etc.)
- An appreciation of security management practices – good protection is unlikely without sound management

DETAILS

Available exclusively to AUSCERT Member organisations.

Delivery Mode

- **Online**: Courses are delivered online via Microsoft Teams , split into two half-day sessions. Participants must attend both sessions to complete the course content.
- **In-person:** On occasion courses may also be conducted face-to-face.

Price

- **Online:** $900 (inc. GST) per person, per training course.
- **In-person:** $1250 (inc. GST) per person, per training course.

REGISTER

Visit our Training page & follow the links: auscert.org.au/training

For any other enquiries please contact: training@auscert.org.au

REQUIRED

A basic knowledge of key IT components and concepts including operating systems, databases, network and client-server computing, applications, management of information technologies and services.

AUSCERT

APPROACH

- Provide a comprehensive perspective on the field of information and cyber security
- Explain the fundamental principles, such as need to know, open design
- A mix of theory and engaging learning experiences including quizzes, and group discussions
- Facilitate opportunities for participants to share experiences and knowledge
- Provide relevant and pragmatic examples of cyber security risk management in practice

CURRICULUM OUTLINE

- Cyber security terminology
- Scope of cyber security objectives – confidentiality, integrity and availability
- Attack trends
- Threat and vulnerability types
- Security principles
- Asset classes
- Attack types
- Malware types
- Security controls, covering technical, procedural and management
  - Key focus on technical – broad scope from networks to systems and cloud
- Security management and planning approaches
- Overview of key security frameworks
- Incident detection and management
- How to stay current