AUSCERT

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.

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

AUSCERT

INTERMEDIATE CYBER SECURITY FOR IT PROFESSIONALS

We rely on the Internet for daily business operations and government service delivery. However, today's threat environment is very different from how it was when many key Internet protocols were designed, resulting in inherent vulnerabilities that require mitigation.

This course is designed to provide participants with awareness of the security issues with a range of Internet oriented technologies and protocols and practical guidance for how participants can secure them.

OUTCOMES

- Enhanced understanding of the security threats and vulnerabilities in key Internet-oriented technologies and mitigation measures
- Understanding of important cyber oriented technologies that would contribute to a cyber security uplift program

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

Basic knowledge of IT, networking and cyber security knowledge including threats, vulnerabilities and risks.

Having completed AUSCERT's Introduction to Cyber Security for IT Professionals is excellent preparation.

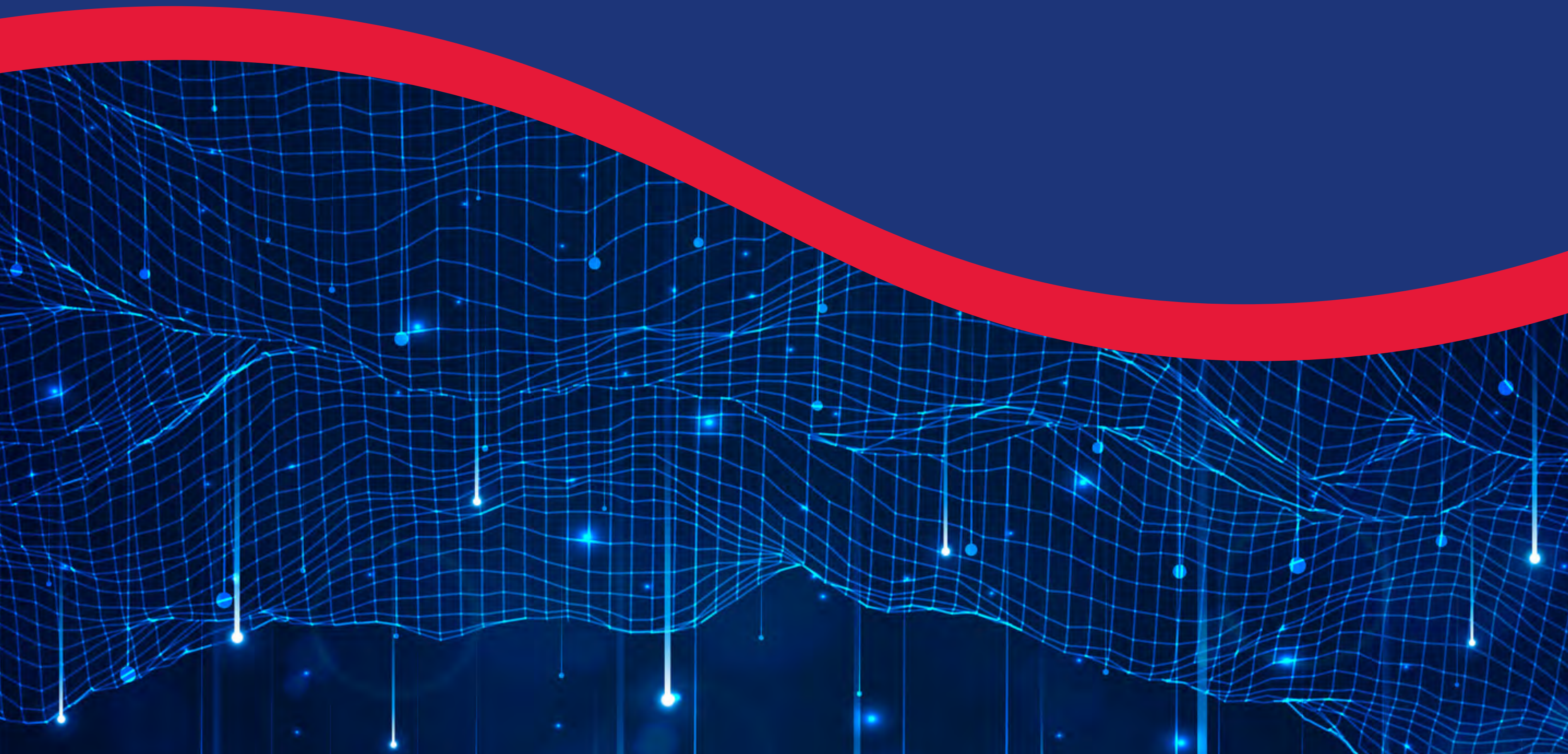
APPROACH

- We describe and discuss how key technologies are abused and bypassed by attackers
- We introduce attendees to the technical and procedural approaches that they can use to thwart attempts to bypass security controls and exploit inherent vulnerabilities
- Incorporating group discussions and interactive learning opportunities
- Reference to and discussion of real-world incidents

CURRICULUM OUTLINE

The curriculum covers key technologies, their inherent weaknesses and the currently available solutions:

- Phishing and Business Email Compromise attacks and the associated email security controls to address them: DKIM, SPF and DMARC
- Domain hijacking, fake web sites, email interception attacks all rely on DNS to be successful. We cover aspects of DNS security that provide important controls to address these threats
- Remote access vulnerabilities and robust configuration choices for Virtual Private Networks (VPNs), including TLS and IPSec security
- TLS security for web sites
- Cryptographic algorithms and protocols – robust options and avoiding weaknesses
- Unix and Linux security – basics of secure system administration
- Introduction to SAN security
- Cloud assurance and due diligence
- BGP hijacking, similar threats, and associated preventative controls



AUSCERT

DATA GOVERNANCE PRINCIPLES AND PRACTICES

This course is designed for a diverse audience, from beginners exploring data governance and its synergy with related initiatives, to those responsible for executing a data governance program, and professionals seeking to understand how effective data governance strengthens cyber security.

The purpose of the course is to provide participants with knowledge about:

- why data governance is important,
- understanding stakeholder data needs and articulating effective data governance approaches,
- integrating data governance techniques with initiatives such as information security, data privacy, and ethics,
- the core components of a data governance framework,
- how to perform data governance ‘by stealth’.

Participants will explore key elements of effective data governance using real-world examples. While we'll reference established frameworks, our emphasis is on practical application.

Upon completion, practical data governance references and templates will be provided to participants.

LEARNING OUTCOMES

- a fundamental understanding of data governance principles
- an understanding of:
  - what level of data governance you need in your organisation
  - how data governance makes data quality management, compliance and cyber security easier
  - how to develop, enable and operationalise a data governance framework
  - enabling your data governance journey through a stakeholder-centric change management approach
  - how to measure success
- skills to develop a data governance roadmap.

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

No specific background knowledge is required. However, a basic understanding of data and information is beneficial.

APPROACH

- Often the best part of training courses are the opportunities for participants to share challenges, experiences and knowledge. We create the environment for this to happen.
- Use of engaging learning modalities including quizzes, polls, small and large group discussions, and practical exercises.
- Highlighting practical pitfalls and opportunities from our experiences.
- Implementing workshop techniques applicable to various scenarios, not limited to data governance, such as turning challenges into organisational objectives.

CURRICULUM OUTLINE

- Data governance framework fundamentals.
- Importance of data governance through case studies.
- Understanding organisational data governance maturity.
- Embedding data governance roles, responsibilities and processes (e.g. data stewards).
- Achieving data governance through established processes that are not typically considered data governance activities.
- Conducting full-lifecycle data risk assessments.
- Collaborating with cyber teams to ensure data is handled safely and securely.
- Addressing rganizational resistance using change management techniques.
- Enabling a mature data culture through literacy and awareness.

AUSCERT

INCIDENT RESPONSE PLANNING

For many organisations, it is not a matter of *'if'* a cyber security incident happens, it is a matter of *'when'*. This course is designed to provide organisations with important information and knowledge to execute one of the critical elements of incident response; preparation.

OUTCOMES

Upon completion of this training session, participants will:

- Understand the NIST 800-61 incident response (IR) phases
- Appreciate the usefulness of cyber security policies and frameworks to IR
- Gain an understanding of the contemporary threat environment
- Design a Cyber Incident Response Plan or modify an existing plan
- Learn to create and tailor cyber incident playbooks
- Be familiar with common online incident analysis tools
- Appreciate the role of tabletop discussion exercises in IR planning and improvement
- Know about open-source tools to self-appraise IR process maturity

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

The level of technical content in this course is low. However, as we cover introductory aspects of threats and attacks, participants will benefit more if they have introductory cyber security knowledge (as taught in the AUSCERT Cyber Security Fundamentals course).

APPROACH

- Emphasis is on empowerment of staff and the importance of collaboration •
- Provides an overview of cyber security incident response planning activities from a practical and pragmatic perspective
- Facilitated opportunities for participants to share experiences and knowledge
- Informative, entertaining and engaging, this course employs videos, quizzes, large and small group discussions and exercises

CURRICULUM OUTLINE

- Introducing incident response – what is it, why do we need it?
- Overview of the NIST 800-61 Incident Response Lifecycle
- The role of Information Security Management Frameworks and Policies in IR
- The contemporary threat environment including an introduction to the MITRE ATT&CK framework
- Design a Cyber Security Incident Response Plan based on the provided template
- Good and bad metrics in cyber security
- IR playbooks – essential elements and examples of best practice
- Building an IR team and self-appraise the IR maturity
- Introduction to common, free, online incident analysis tools

AUSCERT

CYBER SECURITY RISK MANAGEMENT

This course is designed to provide participants the confidence to perform a risk assessment of cyber security risks, the ability to rate, assess and report business risks rather than technical vulnerabilities. Calibrating cyber security as business risks rather than technical vulnerability severity readily facilitates business leader buy-in

OBJECTIVES

- Enhance understanding of how to identify and assess cyber security risks to your organisation
- Management of cyber security risk using standards-based risk management processes
- Integration of cyber security risk management into organisational governance and management processes
- Increase confidence to perform a risk assessment of cyber security risks
- Enable IT and cyber security professionals to liaise with risk professionals to report up to boards and executives
- Use business risk to set priorities for your cyber security improvement program

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

There are no particular background knowledge requirements for this course

AUSCERT

CURRICULUM OUTLINE

- Fundamental risk management terminology and process (ISO 31000 and ISO 27005)
- Application of standard corporate risk management frameworks to cyber security risks
- Techniques for each phase of cyber security risk management:
  - identification
  - analysis
  - evaluation
  - reporting
- Risk management as a framework for sound decision support
- Traps and pitfalls when applying risk management to cyber security risks
- Workshop – put the theory into practice

APPROACH

- Provide a broad perspective on the field of information and cyber security and the relation to risk management
- Facilitate opportunities for participants to share experiences and knowledge
- A mix of theory and engaging learning experiences including quizzes, and group discussions
- Provide relevant and pragmatic examples of cyber security risk management in practice
- Embed learning through practical risk management workshop exercise