ENHANCE YOUR KNOWLEDGE

With our exceptional one day training offerings for individuals and organisations

COSTS

$990 for members
$1980 for non-members

CUSTOMISED IN-HOUSE OR GROUP TRAINING OPTIONS

At **AusCERT** we are also able to develop tailored industry and/or government content with each of our members and clients to ensure that the resulting workshop meets their needs and objectives - P.O.A

FIND OUT MORE

training@auscert.org.au

AUSCERT.ORG.AU

SAFEGUARD YOUR INFORMATION

Don't wait for a security incident.

Act now to proactively protect you and your organisation.

STAY UP-TO-DATE WITH AUSCERT

07 3365 4417
membership@auscert.org.au
auscert.org.au
AusCERT
@AusCERT
/AusCERT

PROUDLY PART OF The University Of Queensland AUSTRALIA

AusCERT Education_

AUSTRALIA'S PIONEER
CYBER EMERGENCY RESPONSE TEAM

AUSCERT EDUCATION

INCIDENT RESPONSE PLANNING

Be equipped with the tools to write a bespoke incident response plan for your organisation

What you will learn:

- Understand NIST Incident response phases
- Self appraise IR process maturity
- Design a Cyber Incident Response Plan
- Learn to create and tailor Cyber Incident Playbooks
- Explain the role of Cyber Security Policies
- Develop an awareness of the top 5 types of Cyber incidents
- Learn the use of and caveats of online tools

Who will benefit?:

- Business and Organisation Executives
- Risk Practitioners
- IT Managers
- Project and Program Managers
- Incident response teams
- Network and system administrators

AUSTRALIA'S PIONEER
CYBER EMERGENCY RESPONSE TEAM

INTRODUCTION TO CYBER SECURITY FOR IT PROFESSIONALS

Understand information security principles, cyber security as a risk to business objectives; and cultivate an appreciation of the current cyber threat landscape

What you will learn:

- The CIA triad
- Security principles, such as need to know
- Overview of major cyber security controls (access control, crypto, network filtering etc)
- Overview of typical threats and vulnerabilities

Who will benefit?:

- Business and Organisation Executives
- Risk Practitioners
- IT Managers
- Project and Program Managers
- Board Directors
- C-level Executives
- IT helpdesk and support staff

MISP

Set-up, configure and integrate Malware Information Sharing Platform into your organisation's cybersecurity defense strategy.

What you will learn:

- How to set up a MISP platform
- What are useful indicators, how to obtain them
- Building an event in MISP
- Distribution communities, Traffic Light Protocol, and connecting to other MISP instances
- MISP API and automation

Who will benefit?:

- IT Managers
- Incident response teams
- SOC teams
- Network administrators
- System administrators

CYBER SECURITY RISK MANAGEMENT

Gain the confidence to perform a risk assessment of cyber security risks and the ability to rate and assess business risks rather than technical vulnerabilities

What you will learn:

- The ability to translate technical vulnerability knowl edge into security risks
- The ability to correlate technically oriented risks into risks analysed against business impacts
- The ability to abstract a myriad of technical security vulnerabilities into a risk assessment audience at a C-level
- The ability to assess cyber risks when agencies out source some operations (e.g. cloud computing)
- The ability to perform on reporting and decision making requirements
- "Quick wins"

Who will benefit?:

- Business and Organisation Executives
- Risk Practitioners
- IT Managers
- Project and Program Managers
- Board Directors
- C-level Executives