Incident Response Planning – Overview

About this Course

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.

Required Background Knowledge

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).

Learning Objectives

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

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