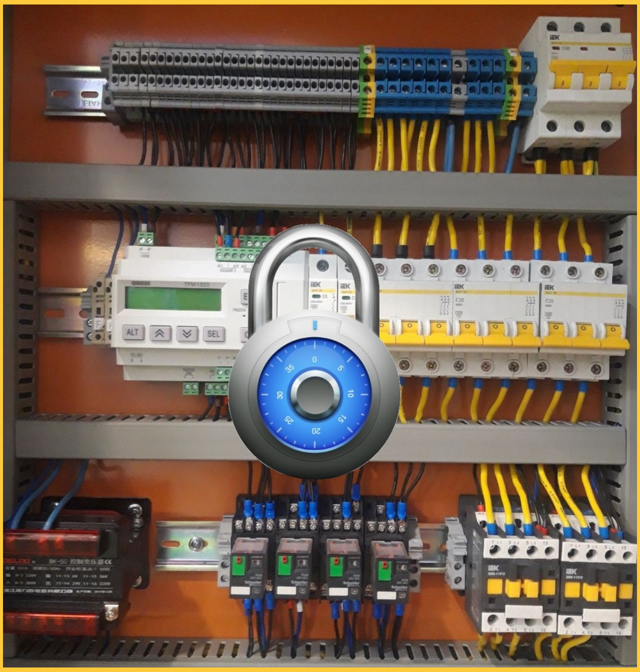
Exercise 7

Incident Management



Dr Diarmuid Ó Briain

Version: 2.0

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

Dr Diarmuid Ó Briain

Table of Contents

This page is intentionally blank

Exercise Scenario

1 Objectives

- To exercise the learners' understanding of incident management principles and practices.
- To identify areas where the learners' knowledge and skills can be improved.
- To develop the learners' ability to work together as a team to respond to an incident.

2 Gas Networks Ireland

Líonraí Gáis Éireann | Gas Networks Ireland

3 Introduction

It's a busy Saturday evening, mid-winter, at the Dublin-based headquarters of Gas Networks Ireland, a major gas supply company serving Ireland. At 22:04 hrs, the company's Supervisory Control and Data Acquisition (SCADA) system detects a sudden drop in pressure in a major gas transmission pipeline in Cork city. The pipeline supplies gas to a significant portion of the city, including residential areas, commercial establishments, and industrial facilities. Your on-call alarm sounds and you are called in to your role within the Operational Technology (OT) Computer Systems Incident Response Team (OT-CSIRT).

Learners are divided into groups of four. Each group is assigned a role to play in the OT-CSIRT:

- **Incident Commander**: Responsible for overall management of the incident response.
- **Technical Lead**: Responsible for leading the technical investigation and response.
- **Communications Lead**: Responsible for developing and implementing the incident communications plan.
- **Documentation Lead**: Responsible for documenting the incident response process and outcomes.

The learners work through the scenario as a team, building and following the Incident Response Plan (IRP) they develop. The facilitator may inject challenges and complications into the scenario to test the learners' skills and knowledge.

4 OT Incident Response Team Resourcing

The learners discuss and document the following:

- How the OT-CSIRT will be organised.
- The roles and responsibilities of each team member.
- Any policies and procedures that need to be established for the OT-CSIRT.

5 Building the Cyber Incident Response Plan

The learners develop a cyber IRP that includes the following elements:

- Overview, goals, and objectives
- Incident description
- Incident detection
- Incident notification
- Incident analysis
- Response actions
- Communications
- Forensics
- Exercising the plan
- System state and status reporting

5.1 Incident Prevention

The learners discuss and document the following:

- Patch management considerations
- Vendor interaction considerations

5.2 Incident Management

The learners discuss and document the following:

- Incident detection methods
- Incident response tools

5.3 Incident Categorisation

The learners discuss and document how incidents will be categorised.

5.4 Incident Containment

The learners discuss and document how incidents will be contained.

5.5 Incident Remediation

- The learners discuss and document how incidents will be remediated.

5.6 Incident Recovery and Restoration

The learners discuss and document how incidents will be recovered from and restored.

5.7 Post Incident Analysis and Forensics

- The learners discuss and document how incidents will be analysed and forensics performed.

5.8 Lessons Learned

- The learners discuss and document any lessons learned from the incident.

5.9 Incident Recurrence Prevention

- The learners discuss and document any steps that can be taken to prevent the incident from recurring.

6 After Action Review

At the end of the tabletop exercise, the facilitator and learners conduct an after action review. The after action review is an opportunity for the learners to discuss what went well, what could be improved, and what they learned from the exercise.

7 Assessment

The facilitator can assess the learners' performance during the tabletop exercise based on the following criteria:

- Understanding of incident management principles and practices.
- Ability to work together as a team to respond to an incident.
- Ability to apply the incident response plan to the tabletop exercise scenario.
- Ability to identify and address challenges and complications.
- The facilitator can use the results of the assessment to identify areas where the learners' knowledge and skills can be improved. The facilitator can then develop additional training or exercises to address these areas.

This page is intentionally blank