Exercise 5

Risk Assessment

Dr Diarmuid Ó Briain

Version: 1.0

Dr Diarmuid Ó Briain

Table of Contents

This page is intentionally blank

Exercise Scenario

1 Objective

The objective of this exercise is for students to understand the nature of risk, identification, mitigation, control and to monitor risks through a risk register.

2 Materials

- Whiteboard or projector
- Markers or pens
- Paper

3 Instructions

1. Divide the students into groups of 4.
2. Give each group a scenario that describes a potential risk to an OT system. For example, the scenario could involve a cyber attack, a natural disaster, or human error.
3. Ask each group to identify the potential impacts of the risk and log in a Risk Register.
4. Ask each group to brainstorm controls that could be implemented to reduce the likelihood or impact of the risk.

4 Group #1 - Cyber attack #1

Assign one example to a group.

- A hacker gains access to the OT system and injects malicious code that causes the system to malfunction. This could lead to a shutdown of critical infrastructure, such as a power plant or water treatment facility.
- A ransomware attack encrypts the data on the OT system, making it inaccessible. The attacker demands a ransom payment in exchange for decrypting the data. If the ransom is not paid, the data may be lost permanently.

5 Group #2 - Cyber attack #2

Assign one example to a group.

- A hacker gains access to the OT system and uses it to launch a distributed denial-of-service (DDoS) attack against a competitor. The DDoS attack disrupts the competitor's operations and causes financial losses.
- A Denial-of-Service (DoS) attack floods the OT system with traffic, making it unavailable to legitimate users. This could disrupt operations and cause financial losses.

6 Group #3 - Natural disaster

Assign one example to a group.

- A flood or hurricane can damage or destroy OT equipment, causing a loss of control over critical infrastructure.
- A power outage can disrupt the operation of OT systems, leading to safety hazards and economic losses.
- A cyber incident can be triggered by a natural disaster, such as a solar flare or a power outage. This could lead to widespread disruption of critical infrastructure.

7 Group #4 – Human Error

Assign one example to a group.

- A human operator makes a mistake, such as entering the wrong data or forgetting to perform a critical step. This could lead to a malfunction of the OT system, with potentially serious consequences.
- A maintenance worker accidentally damages OT equipment. This could also lead to a malfunction of the system.
- A disgruntled employee sabotages the OT system. This could cause widespread damage or even loss of life.

8 Summary

In each of the cyber attack scenarios, the hacker could gain access to the OT system through a variety of ways, such as exploiting a vulnerability in the system's software or hardware, or by phishing an employee. Once the hacker has access to the system, they could inject malicious code, steal data, or disrupt operations.

In the natural disaster scenarios, the damage to OT equipment could be caused by flooding, wind, fire, or other natural hazards. The disruption to operations could be caused by the loss of power, communication lines, or other critical infrastructure.

In the human error scenarios, the mistake could be made by an operator, a maintenance worker, or even a manager. The mistake could be simple, such as entering the wrong data, or it could be more serious, such as forgetting to perform a critical step.

It is important to note that these risks are not mutually exclusive. In fact, they often overlap. For example, a cyber attack could be triggered by a natural disaster, and human error could contribute to a cyber attack or a natural disaster.

By understanding the potential risks to OT systems, organisations can take steps to mitigate those risks and protect their critical infrastructure.

Project:

		Summary			Description				Preventative Actions			Contingency Actions		
ID	Date Raised	Raised By	Description of Risk	Description of Impact	Probability Rating	Impact Rating	Priority Rating	Action	Resource	Date	Actions	Resource	Date

VL = Very Low   L = Low   M = Medium   H = High   VH = Very High