Exercise 5

Frameworks

Dr Diarmuid Ó Briain

Version: 3.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

This page is intentionally blank

Exercise Scenario

1 Objectives

The objectives of this exercise is for learners to:

- Identify the correct framework for a particular scenario.
- Discuss the strengths and weaknesses of each framework.
- Apply the frameworks to real-world situations.

2 Materials

- Whiteboard or projector
- Markers or pens
- Paper

2.1 Scenario

- A Denial-of-Service (DOS) attack on a utility company
- A ransomware attack on a healthcare organisation
- A supply chain attack on a manufacturing company
- A cyberattack on a government agency.

3 Instructions

1. Each learner, within each group of four learners, will be assigned one of the frameworks (ISO 27000, ITIL, COSO, COBIT, or NIST CSF).
2. The learners will then evaluate the company and the scenario presented and assess if the framework, had it been deployed, would help in the scenario presented.
3. Each learner will present their case to the learners in their group and together they will conclude what is the best framework or set of frameworks to apply to their company or organisation.
4. Each group will develop a cybersecurity plan, incorporating frameworks of their choice.

3.1 Group #1 – ESB

ESB has been Ireland's foremost energy company since it was established in 1927, driven by an unwavering commitment to power society forward and deliver a net-zero future for their customers and the communities they serve. URL: https://ww.esb.ie

The company suffered a DOS attack on their network infrastructure in Connacht that has left 750,000 customers without power during the winter.

3.2 Group #2 – Bon Secours Hospital Group

As Ireland’s largest independent hospital group, Bon Secours Health System CLG is renowned for the quality of its service provision coupled with a rich tradition in healthcare. Bon Secours Health System CLG is a not for profit organisation with its mission centred on providing compassionate, world class medical treatment to all those it serves. With 3,000 staff, 450 leading consultants, Bon Secours treats in excess of 280,000 patients annually in its 5 modern acute hospitals in Cork, Galway, Limerick, Tralee and Dublin as well as a Care Village in Cork. It is one of the largest providers of private healthcare in Ireland.. URL: https://www.bonsecours.ie

The group has suffered a ransomware attack on their patient records. The bad actor stopped access to the records temporarily and has uploaded the records of 20 patients on the dark web and promises to release records in batches of 5,000 until the group pays €10,000,000 at which point it will stop and allow the hospital group to regain access to the records.

3.3 Group #3 – MEDITE SMARTPLY

MEDITE SMARTPLY define the standards of engineered wood panels. They deliver exceptionally engineered products, outstanding sustainability credentials, unrivalled innovation and industry leading customer service.

The company have manufacturing sites in Clonmel (MEDITE) and Waterford (SMARTPLY) in Ireland feature the latest production technology to deliver straighter, flatter and more consistent boards than ever before, in a range of sizes and thicknesses unparalleled within the industry. Constant progression and investment have allowed MEDITE SMARTPLY to enter new diverse markets and sectors, meaning that there is always a fresh pipeline of new products to address market demands.

As part of the Coillte Group, the company pride themselves on their sustainable supply chain and manufacturing processes, meaning their products are as environmentally conscious in their make up as they are in their application.

URL: https://mdfosb.com/en

The company suffered a supply chain attack on the Waterford plant, disrupting their Just in Time (JiT) processes and leaving many ordered unfulfilled to their customers across Europe.

3.4 Group #4 – SOLAS

An tSeirbhís Oideachais Leanúnaigh agus Scileanna (SOLAS) is a state agency in Ireland. SOLAS was established on October 27, 2013. Its mandate is set out in the Further Education and Training Act 2013. Among other functions such as research, monitoring and coordinating of further education and training provision, it also advances monies to education and training boards and other bodies engaged in the provision of further education and training programmes. URL: https://www.solas.ie

A cyberattack on the SOLAS Apprenticeship Online website has rendered SOLAS unable to accept new registrations of apprentices or to edit current apprentices. Additionally there is an active threat of personal data of apprentices being released on the public domain after a sample set of 100 names were released as a demonstration of the hackers intentions. URL: www.apprenticeshiponline.ie

3.5 Evaluation

The learners will be evaluated on their ability to identify the correct framework for a particular scenario, discuss the strengths and weaknesses of each framework, and apply the frameworks to real-world situations.

4 Summary

This exercise is designed to help learners to understand and apply five cybersecurity frameworks: ISO 27000, ITIL, COSO, COBIT, and NIST CSF. Learners will have extracted a number of lessons about cybersecurity frameworks from the exercise, including:

- Each framework has its own strengths and weaknesses.
- The best framework for a particular situation will depend on the specific needs of the organisation and the nature of the cyber threat.
- It is often helpful to combine multiple frameworks to create a comprehensive cybersecurity strategy.