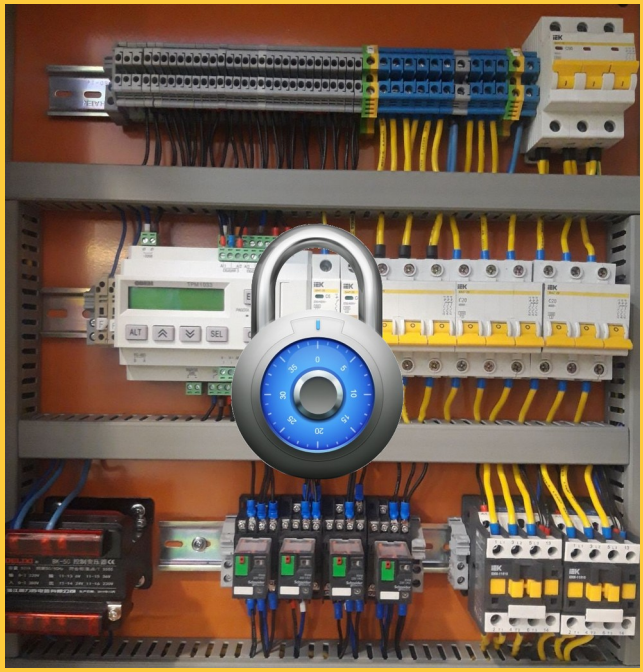
Exercise 8

Legal, Regulations, Compliance and Investigations



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 Objective

- To gain an understanding of the key concepts and issues related to computer crime, intellectual property, liability and negligence, privacy, incident management, and compliance and ethics.
- To develop critical thinking and problem-solving skills.
- To improve communication and collaboration skills.

2 Materials

- Whiteboard or flip chart
  - Markers
- Handouts on each of the following topics:
  - Computer crime
  - Intellectual property
  - Liability and negligence
  - Privacy
  - Incident management
  - Compliance and ethics

3 Procedure

3.1 Introduction (5 minutes)

Briefly introduce the topic of computer crime, intellectual property, liability and negligence, privacy, incident management, and compliance and ethics. Explain the purpose of the exercise.

3.2 Topic Presentation (10 minutes)

- Divide the students into five groups.
- Assign each group one of the six topics.
- Have each group research their assigned topic and prepare a brief presentation for the class.
- Each group should present their topic to the class in 5 minutes.

3.3 Case Studies (20 minutes)

- After the presentations, divide the class back into one group.
- Present the class with a case study that involves all six topics.
- Have the students work together to discuss the case study and answer the following questions:
  - What are the legal and ethical issues involved in this case?
  - What are the potential consequences of the actions taken by the individuals in this case?
  - What recommendations would you make to prevent similar situations from happening in the future?

3.4 Conclusion (10 minutes)

- Lead a class discussion on the key takeaways from the exercise.
- Ask students to reflect on what they have learned.
- Summarise the main points of the exercise.

4 Handouts

Computer Crime

- Computer crime is any crime that involves the use of a computer or the Internet. This can include a wide range of activities, such as hacking, identity theft, fraud, and cyberbullying.

Intellectual Property

- Intellectual property (IP) is a legal term that refers to creations of the mind, such as inventions, literary works, and artistic works. IP rights give the owner of the IP the right to control how the IP is used.

Liability and Negligence

- Liability is a legal concept that means that someone is responsible for something. Negligence is a type of liability that occurs when someone fails to take reasonable care to avoid causing harm to others.

Privacy

- Privacy is the right to be free from unwarranted disclosures of personal information.

Incident Management

- Incident management is the process of responding to and resolving security incidents.

Compliance and Ethics

- Compliance is the act of adhering to laws, regulations, and other requirements. Ethics are the principles of right and wrong that guide our behaviour.

5 Case Studies

5.1 Case Study 1: The Sony PlayStation Network Hack

In 2011, Sony's PlayStation Network (PSN) was hacked, resulting in the theft of personal information from over 100 million users. The hack was a major blow to Sony's reputation and led to a significant loss of revenue.

5.2 Case Study 2: The WannaCry Ransomware Attack

In 2017, the WannaCry ransomware attack infected millions of computers around the world, causing billions of dollars in damage. The attack was a wake-up call for businesses and organizations, highlighting the need for strong cybersecurity measures.

5.3 Case Study 3: The Cambridge Analytica Scandal

In 2018, it was revealed that Cambridge Analytica, a political consulting firm, had improperly obtained personal data from millions of Facebook users. The scandal raised serious concerns about data privacy and the role of social media companies in protecting user data.

5.4 Case Study 4: The Equifax Data Breach

In 2017, Equifax, a credit reporting agency, suffered a major data breach that affected over 147 million people. The breach was a result of a failure by Equifax to properly patch a security vulnerability.

5.5 Case Study 5: The SolarWinds Hack

In 2020, SolarWinds, a software company, was hacked by Russian intelligence agents. The hackers were able to insert malicious code into SolarWinds' Orion software, which was then distributed to customers around the world. The hack was a major security breach that affected thousands of organizations.

5.6 Case Study 6: The Pegasus Spyware Scandal

In 2021, it was revealed that Pegasus spyware, a powerful surveillance tool, had been used to target journalists, activists, and politicians around the world. The spyware was developed by NSO Group, an Israeli company, and was sold to governments around the world. The Pegasus scandal raised serious concerns about the use of spyware and the potential for abuse.