Educate
Engage
Inspire

Module 3

Student workbook

Module 3

Principles of cyber security

Learning objectives

Students will understand:

- Basic cyber security concepts
- Differences between a threat and a vulnerability
- Basic threat types and countermeasures
- Fundamental user security processes

Presented by

In partnership with

The CIA triad

Confidentiality

Integrity

Availability

The 3 goals of information security are to maintain:

- **Information confidentiality**
  Making sure only approved users have access to data.

- **Information integrity**
  Data integrity: assurance that information has not been tampered with or corrupted between the source and the end user.

  Source integrity: assurance that the sender of the information is who it is supposed to be.
- **Information availability**
  Ensuring data is accessible by approved users when needed.

Cyber security activity

Each of the following scenarios will affect the CIA triad in different ways. Explain how in each scenario:

Scenario 1

There are several old users at a company who no longer work there but still have authorised access to files and systems.

C

I

A

Scenario 2

A hard drive with crucial documents was destroyed and nobody had backed the system up in a while. One of the staff said they might have a copy lying around on a USB somewhere at home.

C

I

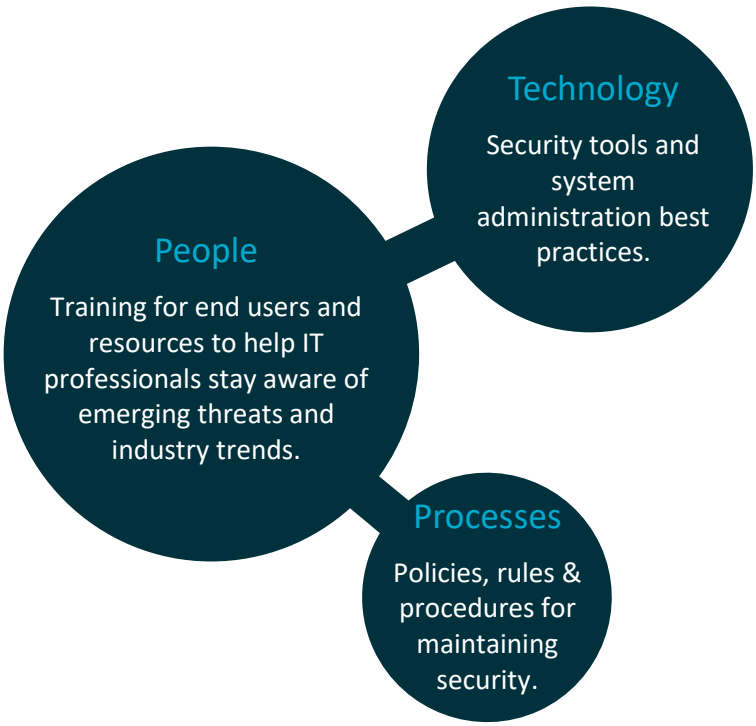
A

Choose one of the above examples and explain how a PPT approach might solve the problem occurring again.

P

P

T



Assessing risk

Threat
An attacker or piece of malware that desires and/or is able to cause harm to a target.

Vulnerability
Flaw in an environment that an attacker can use to harm the target.

Exploit
The method by which an attacker can use a vulnerability.

Risk
The potential that a threat will exploit a vulnerability.

Risk Matrix

		Impact				
		Trivial	**Minor**	**Moderate**	**Major**	**Extreme**
Probability	**Rare**	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

Using the definitions above identify the threat, vulnerability, and method of exploitation in the scenarios below and then use this information to make an assessment using the risk matrix of the level of risk in each scenario.

Scenario 1

A scientist is working on a sensitive document in a public library. Another scientist positions himself at the desk behind her and makes notes on the document to send back to his laboratory.

Threat

Vulnerability

Exploitation

Risk

Scenario 2

A strange email comes through with the title: *Important changes to your system!* You open the email and click on the attachment within the email to try and enact the changes.

Threat

Vulnerability

Exploitation

Risk

Scenario 3

You are in an airport and need to transfer money from one account to another. You search and find free Wi-Fi from an unknown source with no password restriction. You connect to the Wi-Fi and enter your bank account ID and password to open the banking app and complete the transfer.

Threat

Vulnerability

Exploitation

Risk

Password strength

Each of the passwords listed below are varying in their strength. Give each password below a rating from 1 (poor) to 5 (gold standard) and explain why you made that assessment.

Password 1

21november95

Strength

Reason

Password 2

987654321!n

Strength

Reason

Password 3

2:28AQ:AAAaqC2s#30F8gykW

Strength

Reason

Case study – Malware attack

CovidLock 2020

Fear in relation to the Coronavirus (COVID-19) has been widely exploited by cyber criminals. CovidLock ransomware is an example of this. This type of ransomware infects victims via malicious files promising to offer more information about the Coronavirus. The problem is, once installed, CovidLock encrypts data from Android devices and denies data access to victims. To be granted access you must pay a ransom of USD 100 per device to regain access.

What type of online threat is this example?

What vulnerability did this attack target?

How might the victim of this attack be affected?

Learning reflections

Basic cyber security concepts

My understanding of the CIA triad and the PPT approach.

Needs more work **Completely confident**

Threats, vulnerabilities, exploitations, and risks

My understanding of different types of cyber threats and the vulnerabilities they exploit.
My ability to assess the risk these pose in different situations.

Needs more work **Completely confident**

Counter measures

My ability to identify threat types and suggest counter measures to reduce risk in the future.

Needs more work **Completely confident**

User security

My understanding of fundamental user security processes including identification, authorisation, authentication, accounting, and strong passwords.

Needs more work **Completely confident**