7907ICT

Workshop Document

**This document is where you write-up the TEN weekly workshop tasks, each one of which is worth 10% of your total marks.**

# How to Approach these workshops (1 - 10)

This document lays out the ten workshop exercises to be completed each week. Either during the workshop session or at another time at your convenience. It contains detail of the task, plus a read-made template to be used when answering the questions.

This is the document that will be submitted for marking in two stages; Part A in week 6 to include workshops 1 through 5. Part B submitted in Week 11 to include weeks 6 to 10.

Key points to note:

* The output of each workshop is a **600-word written report**.
* Write your 600-word report into this workbook, accumulating them until you have completed all ten, then submit it via the Turnitin portal at the bottom of the assignment page of the course website.
* Don’t be tempted to leave doing the workshop write-up until the week the submission. It is a fact that we usually under-estimate the amount of work needed.
* As per university policy, extensions to the allowed time to submit can be granted with the necessary documentation. But please bear in mind that the IT industry is a very deadline driven profession.
* The workshops follow a similar format. Once you become familiar with the process, you should be able to work through the ten workshops over the duration of the course.
* The workshops can be completed individually or in discussions with groups of 2-4 students. Your submission will be an individual one, not a group submission.
* Ensure your report has clear headings for each.
* Try to do one workshop write-up per week.
* Avoid directly copying and pasting information from online sources, including generative language models like ChatGPT or other.

# Module 9: Assessing Cyber Risk and Insurance Needs

**<Your Exercise Title>**

### Introduction

In today’s digital age, ransomware and malware attacks are a huge threat to businesses, especially for medium-sized manufacturing companies with global operations. These companies often depend on older systems or even use pirate version of operating system software, making them more vulnerable to cyberattacks that could disrupt production, lead to big financial losses, and hurt their reputation. As part of the cybersecurity team, it’s crucial to identify and manage these risks to keep the company’s operations running smoothly and safely. In this report, we’ll focus on one specific cyber risk, how it can impact the business, and what measures can help prevent it. We’ll also look at how cyber insurance can help cover any remaining risk after protections are deployed.

### <potential Risks>

A major risk for a medium-sized manufacturing company is relying on outdated or unpatched systems, which are easy targets for ransomware attacks. Like the WannaCry case, older systems often have security weaknesses that malware can exploit easily, especially in equipment that’s hard to upgrade, like manufacturing machines. If these systems get infected, it could completely stop production, leading to big financial loss. Beyond just losing time and money, the company’s data could be stolen, and customers might lose confidence in the business’s ability to keep their information safe. Overall, this creates a mix of operational, financial, and reputation risks that need to be addressed before hackers take advantage of them.

#### <cybersecurity controls>

To minimize ransomware risks, the company should ensure regular software updates to patch vulnerabilities, or even change operating system in some of their major machines into Linux, which is basically safer than Windows and MacOS, then implement advanced security tools to detect threats early. Regular backups are essential for quick recovery in case of an attack, and employee training on spotting phishing attempts is key since human errors are often the biggest vulnerabilities. Together, these measures provide strong protection against potential threats.

#### <cyber insurance>

Cyber insurance is super helpful for covering any risks left over, even after you’ve put security measures in place. No matter how strong your defenses are, there’s always a chance of getting hurt by an attack, and cyber insurance can help with the financial damage from things like downtime, data breaches, or ransomware. It may also cover legal costs if you need them after an attack. Sometimes, it can even help with ransom payments, though paying ransoms isn’t really a good idea. Basically, it’s a backup plan to handle the costs when security measures aren’t enough to stop an attack.

### Conclusion

In conclusion, protecting a medium-sized manufacturing company from ransomware and malware attacks takes a comprehensive cybersecurity plan. By dealing with risks like outdated systems, putting strong security measures in place, and keeping employees vigilant, the company can greatly lower its chances of being targeted. Cyber insurance is also an important safety measure to cover financial losses in case an attack still happens. Overall, staying proactive, updating security strategies, and being ready for new threats will help keep the company’s operations, data, and reputation secure.

### References

<Use APA referencing style>