Edith Cowan University
School of Science

Computer Security (CSI1101)

Computer Security Vulnerabilities and Countermeasures

Assignment Overview:

This assessment requires you to write a report on a given scenario, which investigates existing security issues (technical and non-technical) and propose countermeasures to overcome the identified vulnerabilities. The scenario has been developed after observing various real-world security weaknesses that organisations face, which cyber criminals can leverage.

This assessment will develop your understanding of analysing security issues and applying the knowledge acquired throughout the semester to provide solutions to these issues. You will also be required to seek guidance from various security forums/manuals such as the 'Australian Government Information Security Manual', ' The Australian Signals Directorate (ASD) Top 35 Mitigation Strategies/ Essential Eight', several 'NIST Standards', SANS resources, and others. References to these resources will be provided through weekly modules. You should also apply feedback from your report assessment to improve your writing skills according to industry standards.

Scenario:

Pines Bay (PB) is a city council in Perth, Western Australia. PB extensively relies on digital services to enhance the accessibility of its services to the residents of the Pines Bay suburb/district and to improve its overall management. As part of its operations, the city collects and processes large volumes of sensitive data, which is digitally processed and stored.

A few months ago, PB fell victim to a triple extortion attack that severely disrupted its working and compromised the aims of security. The council had to pay a hefty sum of money to restore its systems. This incident led to a cyber security audit of PB, revealing critical vulnerabilities that required immediate attention. The audit identified the likely cause of the attack: *"a disgruntled employee was fired from the city, but their IT account was not revoked"*.

The breach sparked community outrage, with residents demanding a comprehensive cyber security audit of PB's systems, operations, and policies to highlight significant grey areas requiring immediate attention. In response, the mayor of Pines Bay City, Josh, ordered a thorough security audit of the existing IT setup, digital culture/operations, and policies to ensure compliance with current cyber security standards.

The city's existing setup, awareness and behaviour are as follows:

a. Every employee at PB uses the city's computer with administrative privileges to undertake their daily routine work.
b. The computers used at PB run the Windows 10 operating system (OS). The OS version being used was released in 2021, running on default settings.
c. PB requires employees to change their passwords every eight months, consisting of a minimum of 5 characters with a mandatory requirement of having one special character in the new password.
d. PB employees are authenticated using password-based authentication.
e. The data is encrypted using the Triple Data Encryption Standard (TDES) with a key length of 168-bit to ensure the relevant aim of security is met.

f. PB uses a web-based application to run its daily operations. The application stores user passwords in the database using the RIPEMD cryptographic hash function.

g. The web-based application is running Secure Socket Layer (SSL) version 1.0.

h. The city disposes of their storage devices after using them for a few years, with data being deleted using software with a single pass.

i. The employees are allowed to work from home and connect to the city's network using the default Remote Desktop Protocol (RDP).

j. No physical security mechanism exists to safeguard the PB's IT systems (end devices and servers). Any employees can enter the PB's server room and access the servers, switches, routers, etc. In addition, due to regular power surges, the site is not conducive to running digital operations.

k. All physical networking and security devices, such as firewalls and intrusion detection systems (IDSs), are being used without redundancy.

Core Tasks:

Josh has approached you to analyse his organisation's current IT setup and practices, along with the security issues discussed above. He wants you to prepare a concise report addressing the following:

Task 1: Identify **six critical** cyber security issues that PB should address as a priority. In devising the security solutions, you should address the following requirements:

a. **Identify** the six critical cyber security issues (**threats and vulnerabilities**) currently faced by PB.

b. **Explain** why your **chosen/identified** six critical cyber security issues **should be addressed immediately**. Justify the potential impact(s) of each identified issue in terms of **Confidentiality, Integrity, and Availability** (CIA) triad.

c. **Application of security solutions: Explain** in detail how you propose to address these six critical cyber security issues. You need to **propose** two solutions for each issue.

d. Identify your **preferred/recommended** solution from your two proposed solutions (in 'c'). Then, **justify** why your **preferred solution** is better than your **alternative** *(i.e., clearly **compare/contrast** your preferred solution to the proposed alternative)*.

> i *Depending on the vulnerability being discussed, a situation may arise where you find it challenging to discuss or find an alternative solution. In such a case, you could attempt this section as a **short-term** vs **long-term** solution where both solutions would be similar, but your proposed implementation would differ with reference to the accrued benefits. You can also propose two versions of the same solution if it is hard to find two distinct solutions to an issue.*

e. Provide a detailed breakdown/**assessment of hardware, software, and training requirements** necessary to implement the preferred solution.

> i *One solution may or may not involve fulfilling all the requirements, i.e., hardware, software, and training. You are only required to outline what hardware, software, and training components are essential to implement your proposed solution (specific brands/models are not needed).*

Task 2: Prepare a comprehensive data backup strategy for PB, enabling the company to recover from future cyber intrusions in the shortest possible time. In doing so, you are to compare/contrast different data backup types available, off-site vs on-site data backup, including the data backup protection. You must provide your recommended strategy (type, site, and protection of data backup) that will benefit PB in the future.

ℹ *Josh has little understanding and knowledge of the prominent threats that could target PB. Therefore, he needs to be convinced that your chosen security issues and the proposed/recommended solutions are most appropriate for PB to run its operations in a secure manner.*

ℹ *Not all solutions need to be technical. Think outside the box about what needs to be rectified within this expanding organisation. There are some **explicit** weaknesses, and a few are **implicitly** mentioned in the given situation. You are allowed to make assumptions on these implicit weaknesses using a separate 'Assumptions' section in your report, but these must be logical.*

See the Required Report Structure and Top Tips/Key Points to Consider sections to ensure you include all required sections and follow the guidelines to score well in this assignment.

Required Report Structure:

Component	**Broad Description and Guidelines**
Title Page	Unit code and title, assignment title, your name, student number, campus and tutor's name
Table of Contents	Generate this automatically. Watch the following video
Introduction	A good introduction provides an overview of the topic, its significance, and the purpose and structure of the report. Some guidelines: • Outline the purpose of the report. • Overview of the given scenario emphasising the current security posture • What did you discover? • Overview of the proposed solutions and how their implementation would benefit the company. • Outline the approach used to undertake your research (databases, security forums, etc.) • Outline of the structure - what are you covering within your report?
Assumptions	*Optional*: Use it if you are making assumptions about the implicit issues in the scenario. The assumptions should have a rationale and be related to the scenario.
Main Content: Task 1 & Task 2 *(Use appropriate headings/sub-headings)*	*Task 1:* • Divide into subsections for each of the six chosen/identified issues. Each component should clearly address the report requirements described in the task outline. Consider the following to address a single issue: ○ Identify and justify the issue in terms of the CIA triad and why it should be addressed immediately. ○ Your proposed/devised solutions, along with an explanation. ○ Your recommended solution and its benefits over the alternative approach(es). ○ Assessment of the hardware, software, and training requirements to implement your proposed solution. *Task 2:* • Include a separate section for the comprehensive data backup strategy covering all requirements. *Think of how you can address some of the above pointers using tables. You may use diagrams/graphs/pie-charts/etc. to reinforce your findings.*
Summary	Briefly draw together the main points raised in the report and summarise your understanding of cyber security's importance for the industry. You should not introduce or discuss any new information. Consider the following: • Inform the reader about the threats and vulnerabilities of the existing arrangements in the organisation. • Consolidate the issues identified with your recommended solutions and essential requirements for their implementation. • Highlight the benefits that will be accrued once the proposed strategy is implemented.

Component	Broad Description and Guidelines
References	• **Acknowledge/support your ideas** and write evidence from sources in your own words using **in-text references** in the body of the report and **end-text references** (reference list) at the end of the report using the APA 7 style. Consider using EndNote. • Aim for 15-20 references as a minimum, including books, peer-reviewed journal articles, published conference papers, white papers, and government and professional organisation reports. You may also use Internet sites (websites and news articles), but they should be reputable. • DO NOT USE WIKIPEDIA; make responsible use of GenAI.

Top Tips/Key Points to Consider:

1. Start early and plan ahead. Use an assignment planner to help you: https://www.studiosity.com/assignment-calculator

2. Read the given case study scenario multiple times and engage with and apply weekly concepts covered in class. This approach will ensure the correct identification of security issues and enable you to find appropriate solutions.

3. Study the marking rubric, paying particular attention to the grade-related descriptors as you will be evaluated against them. If in doubt, ask your lecturer, tutor, or learning adviser before submitting the assignment.

4. Use the structure provided with clear, concise headings. Ideas must flow logically.

5. The style of writing should be appropriate for the purpose, audience and context. Use third-person objective voice, avoiding the use of first-person ('I', 'my', 'we') and second-person ('you').

6. Appropriate discipline-specific terminology and vocabulary must be used in the report.

7. All work should be **referenced** in an academic setting and per ECU policy. Your prior work experience/anecdotal understanding (if any) is valuable in understanding your task. However, you cannot reference anecdotal evidence. When writing an academic report, you must back up your statements using evidence and references that can be verified.

8. When developing your arguments in Tasks 1 and 2, you should aim to **reinforce** your recommendations with books, peer-reviewed journal articles, published conference papers, case studies, and best practices.

9. **Simplify** the communication of your report outcomes. You will lose marks for using complex descriptions or terminology. Use acronyms correctly. Use analogies if they help you communicate the identified issue easily.

10. Sentence structure, spelling, punctuation and grammar should be correct for the report. **Be creative** in how you choose to communicate your findings. Avoid overusing large collections of paraphrased text. Balance the use of text with diagrams, tables and charts. Diagrams can be a much more effective way to communicate ideas or concepts, while tables and charts are helpful in comparing and contrasting different ideas. Whichever you use, ensure you refer to diagrams, tables, and charts in your text, i.e. correctly referenced and/or labelled and referred/discussed in your text.

Common Observations in the Submissions from Previous Semesters:

The following pointers are presented to make you aware of the common mistakes that students have made in the previous semesters. Read and understand all of them to avoid them in your submission.

1. Some students did not apply the feedback given as part of the first report assignment (*Analysis of Contemporary Computer Security Issues*), repeating the same mistakes again.
2. Introduction and Summary sections were poorly written. Specific instructions were given on how and what to include in these two critical sections of the report.
3. The comparison and contrast to alternative solutions lacked proper discussion. In some instances, two solutions were provided, but there was little discussion or justification of why one solution was better than the other.
4. Some alternative solutions did not mitigate the issue/weakness being addressed.
5. Insufficient discussion in relation to the CIA triad.
6. In most cases, students who opted to use the 'Assumptions' section were making assumptions that were explicitly mentioned in the given scenario.
7. Tables and figures were not labelled or given improper headings or not referred to within the discussion.
8. Broken or inaccessible hyperlinks to references.
9. The submissions lacked correct in-text and end-text formatting, according to APA 7th edition conventions. While EndNote was not mandatory, it saves time and allows you to focus on your core work.
10. There were a few surprising submissions where unusual font sizes (16/18) or styles were used as standard fonts. Ensure you use an easy-to-read font (such as Calibri) at size 12.
11. Several submissions had 'Tables of Contents' that were not auto-generated using MS Word. This caused misformatting and inaccuracies within the table. To avoid such problems, watch the following video on how to auto-generate a Table of Contents.
12. The data backup plan was either missing or not attempted by the students.