The University of the South Pacific

School of Information Technology, Engineering, Mathematics & Physics

CS352: Cybersecurity Principles

Semester 1, 2025

Assignment

Weight: 25% (Report 1 - 10% | Report 2 - 15%)

Report 1 Due Date: Friday 25th April 2025, 11:55pm (Fiji Time)

Report 2 Due Date: Friday 23rd May 2025, 11:55pm (Fiji Time)

Learning Outcomes:

- Explain the terminology and key principles associated with cybersecurity
- Analyse cybersecurity risk management techniques to mitigate unacceptable risks.
- Apply viable policies and procedures that support effective cybersecurity protections in the work environment.

Submission

- Submit the two reports in the respective dropboxes.
- **Report 1** is to be done *individually* while **Report 2** is to be done in a *group*.

Declaration

- Please submit a signed declaration for each report to state the work submitted is your own work. The declaration should also include how the assignment scores should be allocated to the individual group members.

There are 2 parts (reports) to this assignment.

Report 1 – Technical Paper – Privacy, Data Breach & Cybersecurity Risks (10%)

Case Scenario: Technical Challenges

In recent years, the frequency of large-scale data breaches has surged, underscoring the urgent need for organizations to prioritize robust cybersecurity measures in order to safeguard sensitive information and effectively mitigate the risks posed by evolving cyber threats.

Keeping the above statement in mind, analyse a large-scale data breach which has happened recently affecting users globally and prepare a technical report for the internal review committee of the organization. Your report has to capture whatever viable policies and procedures that have been incorporated into the organization to provide effective cybersecurity protections and defence strategies.

Your **Report 1** should follow the style of a technical engineering report, intended to be read by a senior executive. Therefore, your report 1 should include the following sections:

- A title page with abstract of no more than 150 words

- A table of contents
- The report 1 body (with appropriate sections such as Introduction, Discussion, Conclusions etc.)
- References (and Appendices if necessary)

In addition, your report 1 should adhere to the following guidelines:

- Align your report to all materials covered in lecture/tutorial up till week 8.
- Ensure your **Report 1** is submitted in electronic form as a word document using the moodle ***Assignment Report 1 Dropbox***.
- Your report 1 length should be 2000 words (+/- 500 words) not including bibliography, appendices, or title page.
- Ensure all sources are cited and a bibliography is included in IEEE style.
- Ensure your work is free from plagiarism and does not breach copyright.

Report 2 – Penetration Testing (15%)

Problem Statement: Penetration testing using Shodan

Use Shodan (https://www.shodan.io/) and carry out a literature review on Shodan. Use the materials uploaded on moodle and do your research on Shodan.

- Create a *free* **shodan account** for your project.
- Carry out some basic searches and see if you can find some nodes with specific content in their banners.
- Prepare a full technical report stating what you have done and results of your penetration testing.

Your **Report 2** should follow the style of a technical engineering report, intended to be read by a senior executive. Therefore, your report 2 should include the following sections:

- A title page with abstract of no more than 150 words
- A table of contents
- The report 2 body (with appropriate sections such as Introduction, Discussion, Conclusions etc.)
- References (and Appendices if necessary)
- In your **Introduction and theoretical background section of the report**, discuss the key principles associated with cybersecurity especially around penetration testing, the scenarios (CLO – 1, 2). Discuss the importance of having viable policies and procedures to support effective cybersecurity protections for the specific discussed scenario (CLO 3)
- In your **discussion section of the report**, discuss your test environment and the vulnerabilities exposed. Discuss this from a cybersecurity risk management perspective (CLO 2) and discuss what viable policies and procedures you would go about implementing for the specified scenario to support effective cybersecurity protections for this specific scenario (CLO3)

In addition, your report 2 should adhere to the following guidelines:

- Ensure your **Report 2** is submitted in electronic form as a word document using the moodle ***Assignment Report 2 Dropbox***.
- Your report 2 length should be 3000 words (+/- 500 words) not including bibliography, appendices, or title page.
- Ensure all sources are cited and a bibliography is included in IEEE style.
- Ensure your work is free from plagiarism and does not breach copyright.

Marking Rubric for Report 1

Area	**CBOK**	**Marks**	**CLO**
Introduction/ Understanding of Principles and the theoretical aspects of cybersecurity (compliance/ law/ ethical behavior)	Communication	2	1
Showing thorough understanding of the scenario/ overview of the most recent data breach	Communication, Societal Issues, IT Governance	3	1, 3
Risk mitigation alternatives/ proposing viable policies and procedures for effective cybersecurity protections and defence strategies	Security Management, Data & Information Management, IT Governance	3	2, 3
Conclusion and Reference		1	3
Overall Presentation of the report		1	
Total		**10**	

Marking Rubric for Report 2

Area	**CBOK**	**Marks**	**CLO**
Introduction	Communication	2	1
Understanding of Principles and the theoretical aspects of penetration testing	Communication, Societal Issues, IT Governance	5	1, 3
Discussion (Results)	Security Management, IT Governance	5	2, 3
Conclusion and Reference		2	3
Overall Presentation of the report		1	
Total		**15**	