Fundamental Concepts of Data Security
ISEC5006

ASSIGNMENT

Due Date: Friday 6-Oct-2022, 12:00pm Perth time
Weight: 30% of the unit mark.

Note: *This document is subject to minor corrections and updates. Announcements will be made promptly on Blackboard and during lectures. Always check for the latest version of the assignment. Failure to do so may result in you not completing the tasks according to the specifications.*

1 Overview

This assignment provides you an opportunity to perform risk assessment for a fictional business. You will need to make use of the relevant data security concepts discussed in the lecture and perform your own research on topics related to the task.

2 The Task

In this assignment, you will play the role of a security consultant. Your client is a fictional organisation. The client has requested you to perform a security risk assessment of the organisation. You are expected to deliver a formal written report which will be presented to the board. It is required that the information security risk assessment is performed in accordance with NIST SP 800-30 Rev.1 - *Guide for Conducting Risk Assessments*

`https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final`

Based on the background information about the company given in Appendix 1, perform the required risk assessment and submit a written report. Note that you may make an assumption on information required to complete the task if it is not described in Appendix 1.

3 The Report

3.1 Structure

The report must be formally written and follow the required structure given below:

- Cover page: It must clearly show your name and student ID and it must indicate to a reader that this is a security risk assessment report for the company.
- Table of contents: Provide a table of contents.
- Executive summary: This must summarise the task and the major findings.
- Introduction
  - Purpose: It must clearly state the reasons for conducting the risk assessment and the objectives that the work aims to achieve.
  - Scope: It must clearly state what are covered and what are not.
- Recommendations: This section must list and explain only the most important findings from the analysis. Typically, they correspond to the items that have the highest risk values as detailed in the risk assessment results subsequently. The recommendations must indicate the vulnerabilities and the possible consequences if they are not immediately addressed. All recommendations need to have correct references to individual items in the risk assessment results.
- Risk assessment approach
  - Participants: You will need to list all people involved in the risk assessment, their roles and contact details.
  - Techniques: You will need to clearly state which methods you use to find out necessary information to identify vulnerabilities, estimate loss, and determine risk values (you must also clearly indicate the information).
  - Risk model: You need to explain in detail which risk assessment approach (qualitative/quantitative) you use. If you use the qualitative approach, you need to clearly indicate the different levels, explain their interpretations, and finally construct the risk matrix that you will follow. If you use the quantitative approach, you will also need to explain the mathematical equations that you use to calculate the risk values. Importantly, all the risk calculations that you present subsequently need to be consistent with the risk model you choose.
- System characterisation: In this section, you will detail all the six components of the information system that you are performing the risk assessment on, including hardware, software, data, procedure, people (or users), and networks. Where applicable, you must show detailed technical information such as model, version, diagrams etc. You should also provide further categorisation for each component for improved clarity.
- Vulnerability statement: In this section, you will list all the vulnerabilities that you have found and briefly describe them.
- Threat statement: In this section, you will identify all possible threat sources. For each threat source, you list possible threat actions they may perform.
- Risk assessment results: In this section, you will assess the risk for each of the vulnerabilities you have discovered above. You must clearly state or make reference to the identified vulnerability, describe the consequent risk, determine the impact and likelihood with justification, evaluate the overall risk, identify the existing control, and evaluate the residual risk. Your risk assessment must address all three security goals: Availability, Integrity, and Confidentiality. Finally, you will recommend relevant control to address the residual risk.
- Conclusion: Summarise the task you have performed, most importantly the findings, and other possible implications of this report.

- References: Include all relevant references that are used in the assessment. The references must follow the Chicago referencing style.
- Appendices: Include additional information that you may have.

3.2 Page Limit

The report must not exceed 30 pages.

Note: Any material beyond the page limit will not be marked.

4 Mark Allocation

The total mark of this assignment is 100, and it is distributed as follows

Submission and presentation as per assignment requirements	10 marks
Overall presentation including table of contents	5 marks
Executive summary	5 marks
Introduction	5 marks
Recommendations	10 marks
Risk assessment approach	5 marks
System characterisation	5 marks
Vulnerability statement	10 marks
Threat statement	10 marks
Risk assessment results	30 marks
Conclusion and references	5 marks

5 Important Information

5.1 Pass Requirement

You need to score at least 30 marks out of 100 marks for this assignment to be considered a reasonable attempt. If you do not achieve this basic pass mark you will fail the unit regardless of how well you perform in the final exam and the average score.

5.2 Submission

☐ The report must be in PDF format and submitted via Blackboard. Use your full name and student ID as the name of the PDF file that you submit, for example

`trump_donald_12345678.pdf`

Submission in Word or any other format is NOT accepted.

☐ A completed and signed 'Declaration of Originality' must also be submitted electronically via Blackboard by the deadline.

5.3 Important Notes

You are required to submit your assignment electronically by Friday 6-Oct-2022, 12:00pm Perth time.

You are responsible for ensuring that your electronic submission is correct and not corrupted. You may make multiple submissions, but only your newest submission will be marked.

6 Academic Misconduct – Plagiarism and Collusion

Please note that this is an individual assignment, what you submit must be entirely your own work except where clearly cited. Mark will be awarded based on your actual work only.

Please note the following, which is standard across all units in the department:

Copying material (from other students, websites or other sources) and presenting it as your own work is plagiarism. Even with your own (possibly extensive) modifications,it is still plagiarism.

If you simply reproduce any parts of the NIST or other risk assessment standards in your work, you still must clearly indicate where they come from.

Exchanging assignment solutions, or parts thereof, with other students is collusion. Engaging in such activities may lead to a grade of ANN (Result Annulled Due to Academic Misconduct) being awarded for the unit, or other penalties. Serious or repeated offences may result in termination or expulsion.

You are expected to understand this at all times, across all your university studies, with or without warnings like this.

Appendix 1 - Case Study Description

IISC Consulting Company Information

IISC is a major consulting firm that provides services to various industries: Finance, Health, Power and Utilities, Retail and Consumer, Government, Mining and CMO Advisory. Its clients range from medium to large organisations, both private and public.

The firm has seven major local offices around the country: Sydney (Head quarter), Canberra, Melbourne, Brisbane, Adelaide, Perth, and Hobart. The centers in Sydney and Melbourne are old heritage buildings located in the CBD. The Brisbane office is a two-storey renovated complex located right on the south bank overlooking the Brisbane river. The other offices are modern multi-level buildings located on the outskirts of the city.

The Sydney and Melbourne offices occupy levels 2-6 of the heritage building. Access to the levels is provided via a public lift. Both offices have the reception on level 2, which also hosts management and finance departments. There is a swipe card access for other levels 3-6. Visitors may obtain a temporary swipe card at the reception and are asked to return it at the conclusion of the visit. The server room is located within level 5 and requires additional keypad access, with the code being only known to authorised ICT support staff.

The Brisbane office has a front reception and a meeting room on the ground floor. Access to the rest of the Brisbane office via the security glass door behind the reception is restricted only to employees presenting a valid swipe card. Two server rooms are located on the ground floor with specialised air-conditioning systems installed at the back of the building.

The other local offices occupy relatively modern 8-level buildings with the first four floors leased to other businesses. Access to levels 5-8 is facilitated by a state-of-the-art facial recognition system. There is no secretary on the ground floor and the only means of communication with staff via an IP-based phone. All visitors need to have their photos taken as part of the access process.

IISC employs over 2000 staff with 10% being high level management, 20% being mid-level management, 10% IT staff and 60% general staff. The recruitment process for the IT staff uses a private HR firm which compiles lists of potential candidates for interviews. The company has an up-skilling program which selects 10% of the IT team every year for training with an emphasis on system administration.

The IT team consists of the main group in Brisbane and local support teams at other branches.

The company has both servers and desktops at every center. The servers mainly use a combination of Windows-based and Linux-based server operating systems, including Windows Server 2019, Windows Server 2016, Redhat Enterprise Linux and Suse Linux Enterprise Server. The Sydney and Melbourne branches also have some servers running Windows Server 2003 for legacy purposes. The workstations use Windows 7, macOS, Linux Ubuntu and Fedora. The company also allows employees to bring their own laptops and tablets to work. Hardware is procured from different vendors.

The server rooms are secured with a keypad mechanism. For the Melbourne and Sydney offices, all confidential data is stored on level 4 whereas other information is stored on the servers on level 5. The Brisbane center stores the backups made for the critical data from all the other centers. For other offices, the server storing confidential data are located on level 8.

Due to the nature of consulting work, IISC allows employees and contractors to work remotely from all over the world. The access to the company's ICT infrastructure is provided via web portal for which a two-factor authentication method is used (password + randomly generated token).

All centers have WiFi networks deployed to augment the wired networks in place. In addition, guest wireless limited access is provided for clients visiting the centers (including the new buildings). The guest wireless is via a token, which can be obtained from the secretarial staff, that allows access for 24 hours to the guest network.

Management and general staff have regular teleconference calls between the offices. Each center has a dedicated meeting room that is equipped with IP-based phones and cameras. The heritage buildings use a typical office format while the new buildings use an open plan layout with only the management having private offices.

IISC has a main website covering the entire company and it is hosted on the cloud by Amazon Web Services (AWS). The main website is managed by a developer which provides regular updates to the site. The company also has an employee dedicated website which provides access to pay and leave information with the content being updated by the same developer.

END OF ASSIGNMENT