Unit:
Network Security and Cryptography

Assignment title:

Escape

Summer 2019

Important notes

- Please refer to the *Assignment Presentation Requirements* for advice on how to set out your assignment. These can be found on the NCC Education website. Click on 'Policies & Advice' on the main menu and then click on 'Student Support'.
- You must read the NCC Education documents *What is Academic Misconduct? Guidance for Candidates* and *Avoiding Plagiarism and Collusion: Guidance for Candidates* and ensure that you acknowledge all the sources that you use in your work. These documents are available on the NCC Education website. Click on 'Policies & Advice' on the main menu and then click on 'Student Support'.
- You **must** complete the *Statement and Confirmation of Own Work*. The form is available on the NCC Education website. Click on 'Policies & Advice' on the main menu and then click on 'Student Support'.
- Please make a note of the recommended word count. You could lose marks if you write 10% more or less than this.
- You must submit a paper copy and digital copy (on disk or similarly acceptable medium). Media containing viruses, or media that cannot be run directly, will result in a fail grade being awarded for this assessment.
- All electronic media will be checked for plagiarism.

Scenario

Escape is a small privately-owned Holistic retreat, established in 2002. Escape provides a wide range of facilities including rooms, restaurants, various therapies and spa treatments. It also includes classes such as Yoga and Pilates.

It is located on a single site and mostly caters for individuals, but businesses are increasingly using it for staff well-being sessions.

The business has grown rapidly and boasts a workforce of more than 80 staff including 10 office/finance assistants; 4 maintenance technicians; 15 therapists and 6 instructors as well as hospitality staff, cleaners and ground keepers.

The retreat runs a LAN, with access to the Internet. The LAN includes servers with financial systems, customer record data and human resources (employee) data.

It is now planning to host a new learning management system (LMS) which will be accessed by staff and will contain training material linked to general competencies relating to their individual role, as well as professional development training which will enable reporting facilities to help track staff training progress.

Staff will be paid for completing training tasks outside of their set working hours, so the system will also record details of when staff log in and use the system.

All staff will require secure access to the LMS from their home PC (via the Internet/ ADSL modem). Many use wireless routers at home and there is a WLAN on site.

Staff connected to the LAN also have access to network folders containing business policies, procedures, committee minutes etc. This is known as the 'Y-drive'. For legacy reasons the retreat hosts its own marketing web site, however, email has recently been switched to the cloud using Microsoft's Office 365.

There have also been growing requests for some staff to have access to the businesses systems (finance, 'Y-drive') from home.

The Managing Director is pleased with the growth of the business, but feels uncomfortable about security, partly because more access is being requested from outside of the business, and partly because of the increasing reports of cyber security attacks. She is also concerned about fines she could receive if there were security breaches.

She has called you in as a consultant to help. Your Terms of Reference are:

To identify the key security challenges faced by the business and recommend solutions.

Task 1 – Risk Assessment -10 Marks

a) Analyse the scenario and identify what you consider to be the 5 most important electronically held information assets in the business. Justify your decision clearly relating it to the Escape scenario. You will need to make some reasonable assumptions here, since the scenario is brief.
This section of the report should be approximately 250 words.

A risk assessment involves the creation of a table of the assets, the threats to those assets and an evaluation of the potential impact of those threats and the likelihood of them occurring. An overall risk value is then calculated for each threat. An example of part of such a table is shown below:

Asset	Threat	CIA?	Likelihood	Impact	Risk
E.g. Student personal data	Server failure	**A**	Low	Medium	Low
	Employee theft	**C**	Low	High	Medium

In the next 3 parts of this task you will systematically create a risk assessment table for this scenario.

b) Create a table which lists the assets. For each asset identify the main security threats that you think could affect its confidentiality (C), integrity (I) or availability (A). Remember, threats can be accidents as well as malicious. There are likely to be multiple threats for each asset and the same threats are likely for several assets.

c) Complete the columns of the table by assessing the **likelihood** of the threat being successful and the **impact** that it would have on the company. In this scenario you should consider Low/Medium and High definitions as follows:

	Likelihood	Impact
Low	Less than once per year	Inconvenience may affect operation for a day or two
Medium	Once per year to once per week	Operation may be impacted for over a week, loss of students.
High	Several times a week	College may not survive – lost reputation and students

d) Now complete the Risk column by using the following Risk matrix.

		Impact		
		Low	Medium	High
Likelihood	Low	Very Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Very High

Task 2 – Controlling the risks – Explanation - 45 Marks

From the table you created in task 1 you should be able to identify the top 13 risks. Once you have identified the highest risks, you need to make recommendations of how to control those risks, i.e. what security you will put in place.

a) Discuss each of the threats you have identified and explain what security you recommend putting in place to reduce the risk. For highest grades you should consider alternatives where they exist and justify your choice. Where you use a technical term, you should explain it.

b) Where you use encryption, explain why and the protocol you recommend.

c) Provide a critical justification of your choices.

This section of the report should be approximately 750 words.

Task 3 – Controlling the risks – Network Diagram - 30 Marks

a) Draw a network diagram, showing network components on the site and employees' connections from home. Each client PC need not be shown, but all other components should be included.

b) Your diagram should include suitable IP addresses together with supporting explanation which states how the network design meets the security requirements.

c) Firewall rules should be listed and explained in a table.

d) Include a 150-word justification stating how and why this applies to Escape's scenario.

This section of the report should be approximately 600 words.

Task 4 – Maintaining Security – 5 Marks

a) Explain any actions you would recommend for ensuring security is taken seriously by the business and for monitoring the effectiveness of the information security management system. Include details of which staff members at Escape should be responsible for security.

This section of the report should be approximately 150 words.

Task 5 Reflective commentary – 10 Marks

You should use this section to reflect on what you learned from completing the assignment.

a) Explain any problems you had and how you went about solving them.
b) Explain anything you would do differently if you were to start it again.
c) Explain if the MD's concerns are justified.

This section of the report should be approximately 250 words.

Submission requirements

- The report should be professionally presented, checked and proof read. In addition, the report should be presented in a format and style appropriate for your intended audience and must relate clearly to the scenario. You must also include a list of references and you must always use correct Harvard referencing and avoid plagiarism throughout your work.

- Your answers to the tasks should be combined in a single word-processed report with an appropriate introduction. The report should be 2000 words +/- 10% in length (excluding tables).

- Familiarise yourself with the NCC Education Academic Dishonesty and Plagiarism Policy and ensure that you acknowledge all the sources which you use in your work.

- All references and citations must use the Harvard Style.
- You must submit a paper copy and digital copy (on disk or similarly acceptable medium).
- Media containing viruses, or media which cannot be run directly, will result in a fail grade being awarded for this module.

Candidate checklist

Please use the following checklist to ensure that your work is ready for submission.

Have you read the NCC Education documents *What is Academic Misconduct? Guidance for Candidates* and *Avoiding Plagiarism and Collusion: Guidance for Candidates* and ensured that you have acknowledged all the sources that you have used in your work?	❑
Have you completed the *Statement and Confirmation of Own Work* form and attached it to your assignment? **You must do this.**	❑
Have you ensured that your work has not gone over or under the recommended word count by more than 10%?	❑
Have you ensured that your work does not contain viruses and can be run directly?	❑