



Unit:

Network Security and Cryptography

Assignment title:

Perfect Pets

Winter 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

Perfect Pets is a small manufacturer of high-quality pet products based in the UK, which sells its products within the UK and Ireland through representatives. The company have a strategy to grow their business and now believe that they should sell their products online directly to customers. Their growth strategy is to sell 75% via an e-commerce site within 18 months.

The Managing Director (MD) is concerned about the security aspects of this approach and the reliance on e-commerce, because of the increasing reports of cyber security attacks. He is also concerned about fines the company could receive if there were security breaches. He is particularly worried about secure payments and ensuring the buyer is genuine.

However, he is aware that there is some legal requirement regarding keeping data confidential both when stored on Perfect Pets systems and during transit across the Internet. He has heard that the way to do this is by using SSL (Secure Sockets Layer) **and encryption**, but he doesn't understand what SSL is or how encryption works. He has also heard about PCI DSS (Payment Card Industry Data Security Standard) but is unsure what their role is.

Furthermore, he is also concerned that customers may be directed to a spoof web site instead of Perfect Pets authentic site and wants to know how they can be sure they are buying from the official site when they send their payment card details.

Current Technology

The company runs a LAN, with access to the Internet via a router. The LAN (Local Area Network) includes a Domain controller running Windows Server 2012 R2 which hosts financial systems (Sage), order processing, customer record data, email (Exchange) and human resources (employee) data. There is a separate file server (Windows Server 2012 R2) which contains design and manufacturing data for their products. Office staff have PCs running Windows 10 professional. All computers have individual host-based firewall and anti-virus installed.

The company has a database-driven dynamic website for product marketing, but this is hosted by their ISP (Internet Service Provider). It has no e-commerce facilities. Marketing staff access the site via a web portal to update the product descriptions on a regular basis.

The inclusion of ecommerce has prompted further requests to enhance the network, and the marketing director has asked for Wi-Fi, so she has greater flexibility to connect to the network and internet from her laptop. However, the MD has not approved the request, so the company will not use Wi-Fi.

The MD has called you in as a consultant to help. Your terms of reference are: *To identify the key security challenges faced by the company and recommend solutions.*

A particular focus should be the additional risks faced by expanding the company to use e-commerce. The company have not decided whether to host the ecommerce infrastructure at the head office, or to use an ISP. You should advise them on that from a security perspective.

Task 1 – Risk Assessment - 10 Marks

As a security professional, you point out that the most effective approach is to start with a risk assessment, so that the most valuable information assets can be prioritised. This ensures that security measures are put in place in the most cost-effective way.

- a) Analyse the scenario **and** identify what you consider to be the FIVE (5) most important electronically held information assets in the company. Justify your decision. You will need to make some reasonable assumptions here, since the scenario is brief.

This section of the report should be approximately TWO HUNDRED AND FIFTY (250) words.

- b) Create a table (see below) 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. You should complete columns labelled Asset (a), Threat (b) and CIA? (b) only for this question.

Asset (a)	Threat (b)	CIA? (b)	Likelihood (c)	Impact (c)	Risk (d)
E.g. customer personal data	Server failure	A	Low	Medium	Low
	Employee theft	C	Low	High	Medium

- 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. You should now complete columns labelled Likelihood (c) and Impact (c) only for this question. 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

It is, of course possible to have Low Likelihood **and** High Impact – the columns are not related.

- d) You should now complete the final column labelled Risk (d) only for this question using the following Risk matrix.

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

Task 2 – Controlling the risks – Explanation - 45 Marks

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. Some controls will be technical, others will involve policies or management actions.

- a) Discuss each of the threats you have identified **and** explain what security you recommend to reduce the risk. For the highest grades you should consider alternatives where they exist **and** justify your choice. Where you use a technical term, you should explain it.
- b) There will be a need for encryption **and** you should explain why you recommend it **and** state the protocol **or** encryption algorithm that you recommend. You should discuss the statement made by the MD asking if 'SSL and encryption' solves the problem that he identifies.

This section of the report should be approximately SEVEN HUNDRED AND FIFTY (750) words.

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

The scenario provided an outline of the main network components, excluding printers, switches and client PCs. The existing system has security vulnerabilities **and** your risk assessment should have identified methods of controlling the risks. You now need to prepare a diagram to show how to secure the network. Make sure you are clear where the ecommerce software **and** hardware are located. If you select an ISP to host it, show this clearly in the cloud.

- a) Draw a network diagram, showing network components of the company **and** new e-commerce system. Each client PC need not be shown, but all other components should be included.
- b) Your diagram should include suitable (invented, but realistic) IP addresses.
- c) Make sure that you explain how the network design meets the security requirements that you identified in Tasks ONE (1) & TWO (2). Any alternatives should be briefly discussed.

This section of the report should be approximately FOUR HUNDRED AND FIFTY (450) words.

Task 4 – Maintaining Security – 8 Marks

Security is a process, not a one off task, so you need to explain how security will be maintained in the future.

- a) Explain, **with reasons**, any actions you would recommend for ensuring security is taken seriously in the company **and** monitoring the effectiveness of the Information security management system.

This section of the report should be approximately ONE HUNDRED AND FIFTY (150) words.

Task 5 Reflective commentary – 7 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.

This section of the report should be approximately ONE HUNDRED AND FIFTY (150) words.

Submission requirements

- The report should be professionally presented, checked and proofed. In addition, the report should be presented in a format and style appropriate for your intended audience. 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 1750 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?

☐