Unit:
Network Security and Cryptography

Assignment title:
Star Shredding

September 2018

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

Star Shredding is a rapidly growing company, which is based in Birmingham (UK). The company provides a professional shredding service for homes and offices, both within the UK and in Europe. Established as a family business in 1982, *Star Shredding* has grown from a local and regional business to a national company that specialises in shredding confidential documentation. With approximately 60 staff, *Star Shredding* has two regional offices in Bristol and Newcastle. All three sites offer an onsite shredding facility. The company is ambitious and views shredding as a good financial opportunity.

Regrettably, the senior management team of *Star Shredding* does not fully appreciate information security risks for their own business or the measures required to control them. Moreover, the company has limited financial and technical resources, and any IT developments must fit within a tight budget.

Star Shredding have recently employed you as an IT manager. In your first week, you notice the following problems:

- There are no company policies in relation to information security;
- The company has not considered the issue of ownership of information and data, and corresponding access rights;
- The IT infrastructure is disjointed in nature with several servers of various ages running different systems (e.g. Accounts system, *Shreddware* logistics system, Domain controller for user authentication);
- There are common system failures both in relation to hardware and software, which in turn, have caused significant delays;
- Some users have received phishing emails and have downloaded viruses;
- The email is not hosted by an ISP, but on a server running MS Exchange in the LAN.

In addition to these problems, your initial discussions with the Managing Director reveal that he has little understanding of networks and computing in general. You have experience with ISO27001, and whilst this is the primary international standard for Information Security Management, it requires a large amount of work and may be too expensive to implement.

You've recently looked at two less onerous approaches to information security: the UK Government's 'Cyber Essentials' programme and '10 steps to Cyber Security' guidance from CESG. However, these appear quite basic. Another approach is a business focus, promoted in ISACA's Business Model for Information Security (BMIS).

Current Technology

The company runs LANs in each office, with access to the Internet via a router. The Head Office LAN 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 runs the *Sheddware* logistics system and integrates with Exchange (the reason that the company hosts their own email server). Office staff have PCs running Windows 7 Professional. All computers have individual host-based firewall and anti-virus installed.

The company has a content management system (WordPress) website for marketing with a contact form and blog, which is also hosted at the head office. Marketing staff access the site via a web portal and update the news and blog on a regular basis.

Each office has a Wi-Fi system, and regional offices connect directly to the headquarters. Regional offices do not host any systems other than client PCs and a small Domain Controller for authentication. Sales staff often visit client premises (domestic or business) to scope work and provide quotations. The company has recently implemented an online system so that sales staff can remotely access systems via a Microsoft Surface 3 Tablet.

As the IT Manager, your Managing Director has asked you to advise how best to protect the company's data. 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 will need to advise them on this issue 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 FIVE (5) important electronically held information assets relating to *Star Shredding*.

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.

Asset	Threat (b)	CIA? (b)	Likelihood (c)	Impact (c)	Risk (d)
E.g. customer 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. 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 customers.
High	Several times a week	Company may not survive – lost reputation and customers

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

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

A completed table will look something like this:

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

Task 2 – Explaining Risk Control (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 be put in place 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) Briefly discuss the relevance of the recommendations of Cyber Essentials, the '10 steps to Cyber Security' and BMIS.

c) Where you use encryption, explain why you recommend it and also state the protocol or encryption algorithm that you recommend.

This section of the report should be approximately 750 words.

Task 3 – 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 software and hardware are located.

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 1 & 2. Any alternatives should be briefly discussed.

This section of the report should be approximately 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. Explain any actions you would recommend for ensuring security is taken seriously in *Star Shredding* and monitoring the effectiveness of the Information security management system.

This section of the report should be approximately 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 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 1500 words +/- 10% in length (excluding tables).
- All references and citations must use the Harvard Style.
- You must submit a paper copy and digital copy (on disk or similarly acceptable medium).

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?	❑