Unit:
Network Security and Cryptography

Assignment title:
Turing Hill Fire and Rescue Service

December 2015 – Sample Assignment

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

Turing Hill Fire and Rescue Service (THFRS) protect the large town of Turing Hill. During the last five years, it has an active policy of exploiting new technology as a way to improve efficiency and ensure safety for its officers.

Information about commercial properties that can be used to establish safety and fire risks is collected from a variety of sources, which include surveys conducted by fire officers, documents outlining fire protection measures already put in place, and Computer Aided Design (CAD) drawings of premises. This information is critical to establish the risks should a fire occur at the premises and it held at the THFRS Data Centre. It is clearly vital that such information is not out of date.

Each fire engine carries a Mobile Data Terminal (MDT) which provides (offline) access to the key risk information and standard operating procedures for the fire type. The MDT is synchronised with the THFRS Data Centre while the fire engine is situated in its base fire station through Wi-Fi.

Senior officers take charge of larger incidents, and there is a requirement for them to have access to this risk critical information at the scene of incidents together with access to standard operating procedures. This information was carried in paper form in a fire officer's vehicle. Yet this manual system caused difficulties in ensuring information was current and the volume of material carried also posed difficulties for rapid access.

A new system is to be introduced, where senior officers have mobile devices, connected through a 4G mobile phone network to provide real-time access to data held on THFRS network via Microsoft SharePoint. This enables officers to be fully informed of necessary information whilst they are managing the incident and ensures information is up-to-date. After consultation with business users, the mobile device selected was the Apple iPad, though this was not the preference of the ICT department.

You are the newly appointed Chief Information Risk Owner for THFRS and you are concerned about the additional risks that will occur when using this mobile platform. Your discussions with your new colleagues and your boss give you a fair amount of confidence that security is taken seriously.

However, you decide that it would be sensible to not only check that the THFRS is using appropriate security for its current operation, but also extend its security coverage to include the new mobile system since iPads will be used to access potentially sensitive data in real time over a 4G network. Crucially, mobile devices will also be employed for usual day-to-day business functions including email and calendar, in addition to personal use. As Chief Information Risk Owner, you are required to complete a series of tasks covering risk assessment, risk control and maintaining security.

Tasks are on next page

Task 1 – Risk Assessment (10 Marks)

a) Analyse the scenario and identify FIVE (5) important information assets relating to THFRS.

b) Create a table which lists the assets. The table should be structured in the same way as the one shown below. 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.

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

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 THFRS. 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 less than a day.
Medium	Once per year to once per week	Operation may be impacted between 1 day and a week – slowing response to incidents to a limited extent.
High	Several times a week	Data Protection fine or inability to access essential data to deal with an incident.

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

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

For example, a completed table for an asset should look like:

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

Tasks continue on next page

Task 2 – Explaining risk control (45 Marks)

Once you have identified FIVE (5) risks, you need to make recommendations of how to control these risks, i.e. what security you recommend.

a) For each risk, explain what security measures you would recommend to put in place to reduce the threat. A good answer should discuss a range of security measures to combat a threat and then provide a justification of your choice. You should also explain technical terms in your answer.

b) Explain any use of encryption and the protocols you would recommend to combat a risk.

This task requires approximately 750 words.

Task 3 – Network Diagram (30 Marks)

a) Draw a network diagram that shows connections to networking equipment such as firewalls, servers, PCs, routers at the command (data) centre. You should include remote connections to fire stations and mobile connections to senior officers and fire engines. However, each client PC should not be shown and you only need include ONE (1) example of a fire station, mobile officer and fire engine with MDT.

b) Your diagram should identify where public and private IP addresses are used and if Network Address Translation (NAT) is used you should identify the type and where it takes place. You should provide an explanation which states how the network design meets the security requirements.

c) List and briefly explain any Firewall rules.

This task requires approximately 450 words plus a diagram

Task 4 – Maintaining Security (5 Marks)

Explain any actions you would recommend for monitoring the effectiveness of the Information Security system.

This task requires approximately 150 words.

Tasks continue on next page

Task 5 – Reflective commentary **(10 Marks)**

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

a) Explain any problems you had and how you went about solving them.
b) Discuss lessons learned during completion of the assignment.
c) Explain anything you would do differently if you were to start it again.

This task requires approximately 150 words.

Guidance and submission requirements

- Your answers should be professionally presented, checked and proofed. In addition, it 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 should be word-processed and total 1500 words in length (+/- 10%) You will lose marks if you go under or over this word count.
- 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? □