# Unit:
# Network Security and Cryptography

## Assignment title:

## Together Trust

## December 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

*Together Trust* is a charity that specialises in Cancer treatment and is based in a Hospital in Nottingham, UK. The aim of the Trust is to provide the finest treatment possible to its patients in a relaxed, clinically safe and pleasant environment. The *Together Trust* is approved by the UK Care Quality Commission for the provision of consultations, diagnostic tests, therapies and surgical treatments as day patients. The Trust is also recognised for the treatment of UK National Health Service (NHS) patients.

In 2015 new satellite *Together Trusts* were established in Salisbury and Windsor which all provide facilities for consultations, some diagnostic tests and therapies. The main *Together Trust* in Nottingham is the hub day care hospital providing a comprehensive range of diagnostic tests, various radio and chemo therapies, and a fully equipped operating theatre suite to support the satellite centres.

The Trust has permanent staff employed as administrators, consultants, therapists and nurses, but all specialist surgery is carried out by independent Surgeons through specific contracts. Surgeons are typically at a Trust for 1 day per week.

The Trust has recently suffered a ransomware attack, which encrypted much of the data on their network and meant that they were unable to operate for almost a week. In the end they decided to pay the ransom as it was more cost effective than attempting to recreate the system from patchy and old backup data.

The CEO has therefore called you in as a consultant to ensure that this does not happen again, and now states that information security is 'top priority'.

In your discussions with the senior managers, including the IT manager (who seems to have been blamed for all security issues), you discover that:

- Some users have received phishing emails and have downloaded viruses;
- There are no company policies in relation to information security;
- The company have not considered the issue of ownership of information and data, and corresponding access rights;
- The email is not hosted by an ISP, but on a server running MS Exchange in the LAN, though the company website is hosted by the ISP;
- Patients are allowed to browse the internet via 'free' Wi-Fi at Trusts.

The CEO has been looking to identify 'best practice' and has discovered ISO27001, the Government's 'Cyber Essentials' programme and '10 steps to Cyber Security' guidance from the 'National Cyber Security Centre'. He is not sure of the difference but likes the idea of adhering to an international standard. Given other high-profile security breaches in the healthcare sector, he considers that certification may give them a business advantage. Furthermore, contracts with the publicly funded NHS would be cancelled without an appropriate information security management system.

### Current Technology

The company runs LANs in each Trust, with access to the Internet via a router. The Nottingham Office LAN includes a Domain controller running Windows Server 2012 R2 which hosts financial systems (Sage), order processing, patient record data, email

(Exchange) and human resources (employee) data. Specialist equipment for photographing eyes is also linked to the 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 by their ISP. Marketing staff access the site via a web portal and update the news and blog on a regular basis.

Each Trust also has a Wi-Fi system, and regional Trusts connect through the Internet to the headquarters.  Regional Trusts do not host any systems other than client PCs and small Domain Controller for authentication.

As the InfoSec consultant, 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 the company as a breach of confidential patient data could cause the company to close since they would be liable for a fine up to €20 million or 4% of global turnover, whichever is highest.

## 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.

This section of the report should be approximately 250 words.

**a)** Analyse the scenario and identify FIVE (5) important electronically held information assets relating to *Together Trust*.

**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 (a) | Threat (b) | CIA? (b) | Likelihood (c) | Impact (c) | Risk (d) |
|---|---|---|---|---|---|
| E.g. patient 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. 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 patients. |
| **High** | Several times a week | The trust may not survive – lost reputation and patients |

**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. patient 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 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 ISO27001.

**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. 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 the company 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 1750 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? | ❑ |