

**NETWORK SECURITY AND CRYPTOGRAPHY**

**Module Title**

**SMITH AND JONES AUCTIONS**

**Assignment Title**

**AUTUMN 2020**

**Examination Cycle**

**PYAE THUTA**

**Candidate Name**

**00185308**

**Candidate No**

**KMD Computer Centre (Yangon)**

**Centre Name**

**30-JUNE-2020**

**Submission Date:**

**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 *Campus*. Scroll down the left hand

side of the screen until you reach Personal Support. Click on this, and then on Policies and

Advice. You will find the Assignment Presentation Requirements under the Advice section.

* You must 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. The

policy is available on *Campus*. Follow the instructions above, but click on Policies rather

than Advice.

* You must complete the **‘Statement and Confirmation of Own Work’**. The form is

available on the Policies section of *Campus*. Scroll down the left hand side until you reach

Personal Support. Click on this and then click on Policies and Advice.

* Please make a note of the recommended word count. You could lose marks if you write 10%

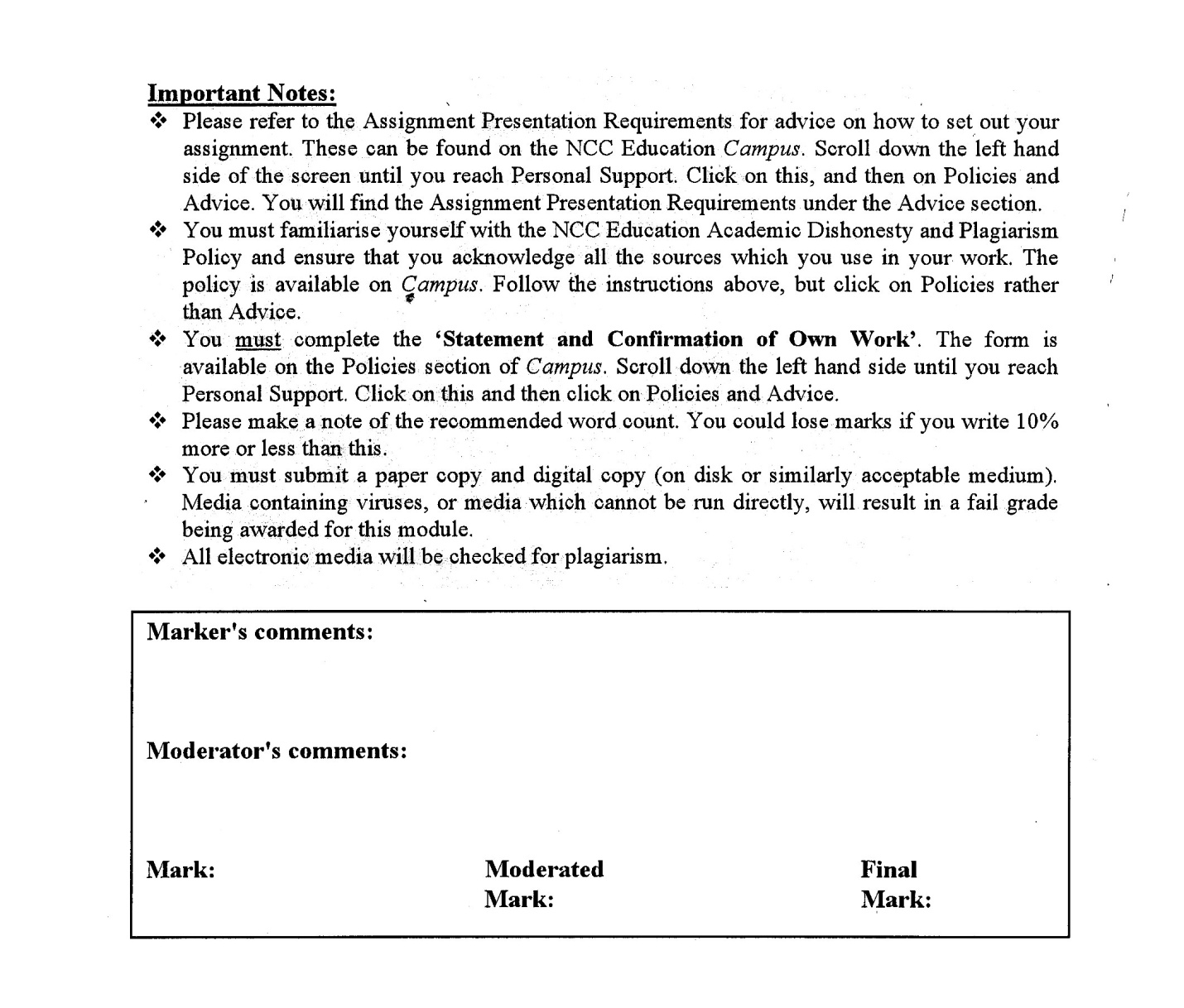
more or less than this.

* You must submit a paper copy and digital copy (on disk or similarly acceptable medium).

Media containing viruses, or media which cannot be run directly, will result in a fail grade

being awarded for this module.

* All electronic media will be checked for plagiarism.



****

**Statement and Confirmation of Own Work**

**Programme/Qualification name: L5DC**

*All NCC Education assessed assignments submitted by students must have this statement as the cover page or it will not be accepted for marking. Please ensure that this statement is either firmly attached to the cover of the assignment or electronically inserted into the front of the assignment.*

**Student declaration**

I have read and understood NCC Education’s Policy on Academic Dishonesty and Plagiarism.

I can confirm the following details:

**Student ID/Registration number : 00185308**

**Name : PYAE THUTA**

**Centre Name : KMD Computer Centre (Yangon)**

**Module Name : Network Security & Cryptography**

**Module Leader : HEIN SITHU NYUNT**

**Number of words : 1909**

I confirm that this is my own work and that I have not plagiarised any part of it. I have also noted the assessment criteria and pass mark for assignments.

**Due Date : 30-JUNE-2020**

**Student Signature :** thuta

**Submitted Date : 30-JUNE-2020**

**Table of Contents**

[Introduction 5](#_Toc48213768)

[TASK (1) Risk Assessment 8](#_Toc48213769)

[a) 5 most important electronically held information 8](#_Toc48213770)

[The 5 most important electronically held information in the business are as follow. 8](#_Toc48213771)

[ Bidding Items Information 8](#_Toc48213772)

[ Customer Information 8](#_Toc48213773)

[ Staffs Information 8](#_Toc48213774)

[ Payment Information 8](#_Toc48213775)

[ Ecommerce data 8](#_Toc48213776)

[b) Threat Identification 9](#_Toc48213777)

[TASK (2) Controlling the Risks 11](#_Toc48213778)

[Ransomware 11](#_Toc48213779)

[Eavesdropping 11](#_Toc48213780)

[DDOS attack 12](#_Toc48213781)

[Botnet 12](#_Toc48213782)

[Computer Virus 13](#_Toc48213783)

[Employee Theft 13](#_Toc48213784)

[Trojan Horse 14](#_Toc48213785)

[Phishing 14](#_Toc48213786)

[Server Failure 14](#_Toc48213787)

[Man in the Middle 15](#_Toc48213788)

[a) Why encryption is necessary 16](#_Toc48213789)

[Task 3 - Setting up the VPN 19](#_Toc48213790)

[a) Differences between Intranet and Extranet 19](#_Toc48213791)

[Benefits of Intranet 19](#_Toc48213792)

[Benefits of extranet 20](#_Toc48213793)

[Recommendation 21](#_Toc48213794)

[b) Network Diagram for “Smith and Jones Auctioneers” 21](#_Toc48213795)

[c) Security features of using VPN firewalls 22](#_Toc48213796)

[Unified Thread Management (UTM) 22](#_Toc48213797)

[Deep Packet Inspection (DPI) 22](#_Toc48213798)

[Intrusion Prevention System (IPS) 22](#_Toc48213799)

[Next General Firewall (NGFW) 22](#_Toc48213800)

[Rule of firewall 22](#_Toc48213801)

[Task 4 – Maintaining Security 24](#_Toc48213802)

[ Training 24](#_Toc48213803)

[ Setting Policies for business 24](#_Toc48213804)

[ Vulnerability assessment 24](#_Toc48213805)

[ Network security Audit 24](#_Toc48213806)

[ Contracts and user acceptance check box 24](#_Toc48213807)

[Task – 5 26](#_Toc48213808)

[Analysis 26](#_Toc48213809)

[Action Plan 26](#_Toc48213810)

[Future Development 26](#_Toc48213811)

[References 27](#_Toc48213812)

[Candidate Checklist 30](#_Toc48213813)

**Introduction**

# Introduction

“Smith and Jones Auctioneers” is a world’s largest industrial auctioneer conducting hundreds of used heavy equipment. Auctions are held at more than 60 auction sites in different regions. Online participation is made by more than half of bidders (Customers).

The company’s most important requirement is fast network and free infections. The company needs to handle “Malware” that can disturb the bidders who bid online and can expose sensitive business’s data. The company have to make sure that the bidding information are safe and secure for customers. There may be malicious websites links which users may accidently click. These links are one of the common sources of infections which are trying to prevent with the use of “Web Filtering Application” by the company. But the prevention has a trouble because routing traffic from all 60 auction sites to one main location is slowing down the critical business application. In addition, “Smith and Jones” decided to make every site can access internet with its own internet connection but there must be only one central web security control for all auction sites.

Moreover, the “Smith and Jones” wants to make sure that all auction sites can confidently offers guests with Wi-Fi access for browsing the web with their devices. The company intends to connect at least 500 people over Wi-Fi at the same time.

**Key Challenge for “Smith and Jones”**

* The company wants to add new auction sites in Manchester City and Mexico City. These sites must be prototypes for all other auction sites.
* All auction sites must be connected through main site in Toronto, Canada.
* To prevent network outages and protect all sensitive information.
* The employees and customers must be provided with great experience.
* Workload must be minimized for a small IT team.
* Offer a Site Security Solution
* WAN performance should be improved.
* Wi-Fi BYOD (Bring Your Own Device) systems should be identified and designed.

(NS&C Assignment: Smith and Jones Auctions , 2020 )

**Task - 1**

# TASK (1) Risk Assessment

## 5 most important electronically held information

## The 5 most important electronically held information in the business are as follow.

1. Bidding Items Information
2. Customer Information
3. Staffs Information
4. Payment Information
5. Ecommerce Data

### Bidding Items Information

The bidding items are directly sold to customers. Therefore, the detail information such as price, weight, company name. etc. are need to stored carefully.

### Customer Information

The name, address and contact number of customers(bidders) must be held because this information will be necessary when customers make payment.

### Staffs Information

The company run with many staffs of different roles. So, each staff role and staff information such as contact number, name, etc. have to be held carefully.

### Payment Information

Information such as card number, total amount, etc. are stored when customers makes payment. This information is sensitive and needed to stored carefully.

### Ecommerce data

The ecommerce website data such as transaction tracking data for “Smiths and Jones” ecommerce website is also sensitive for the business.

(Spacey, 2017)

# Threat Identification

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | CIA? | Likelihood | Impact | Risk |
| Bidding Items Information | Botnet | I/C | Medium | Medium | Medium |
| Ransomware | A | Medium | Medium | Medium |
| Server failure | A | Low | Medium | Low |
| Employment Theft | C | Medium | Medium | Medium |
| Virus | A | Medium | Medium | Medium |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | CIA? | Likelihood | Impact | Risk |
| Customer Information | Server failure | A | Low | Medium | Low |
| Man in the middle | C\I | Low | Low | Very Low |
| Phishing | C\I | Medium | Low | Low |
| Ransomware | A | Medium | Low | Low |
| Employee Theft | C | Medium | Medium | Medium |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | CIA? | Likelihood | Impact | Risk |
| Staffs Information | Trojan Horse | C\I | Low | Medium | Low |
| Phishing | C\I | Low | Low | Very Low |
| Server failure | I | Medium | Low | Low |
| Virus | A | Low | Low | Very Low |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | CIA? | Likelihood | Impact | Risk |
| Payment Information | Ransomware | A | Medium | Medium | Medium |
| Botnet | C\I | Low | Medium | Low |
| Phishing | C | Low | Low | Very Low |
| Eavesdropping | C | Medium | High | High |
| Employee Theft | C | Low | Medium | Low |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | CIA? | Likelihood | Impact | Risk |
| Ecommerce data | DDoS Attack | A | Medium | Medium | High |
| Ransomware | A | Medium | Medium | High |
| Phishing | C | Low | Medium | Low |

(Baylor, 2018)

(Melnick, 2018)

**Task - 2**

# TASK (2) Controlling the Risks

The following possible risks are listed below to control the highest risks within the business network.

### Ransomware

Hackers attack database system of a business by encryption data or deleting data during ransomware.

**Ways to protect Ransomware**

* Using Firewall
* DMZ

(Anon., 2020)

* Encryption of important data

**Recommendation**

Implementing DMZ is the most suitable method for “Smith and Jones Auctioneers” because DMZ can provide detection within the system and control permission access. The services provided by DMZ help to the safety of internal database in the business which stores sensitives data.

### Eavesdropping

Attackers can attack the connection between business and the customers, then they receive the data secretly. This is harmful for the business because the payment data and customer data are sensitive.

**How to protect Eavesdropping**

* Encryption of data
* Antivirus software
* Using Firewall

**Recommendation**

Business should encrypt all the sensitive data like credit card number, customer contact number, bidding items information. This can help customers to communicate confidently with the business.

### DDOS attack

DDoS attack is where cyber criminals disturb the website traffics or server making the website unavailable to users.

(Annonymous, 2020)

**How to protect DDOS attack**

* Using firewall
* Using VPN
* DMZ

Recommendation

Using firewall is the most suitable solution for DDoS attack. Each option sites of the business should use firewall to prevent the website and sensitive data.

### Botnet

Some hackers infect the hardware devices and control these devices to do malicious activities. (Anon., 2020)

**How to protect Botnet**

* Using Antimalware software

(Rouse, 2017)

* Firewall

(Anon., 2020)

* Patch Management

(Anon., 2017)

**Recommendation**

Firewall is the most suitable method to protect the business from Botnet Attack. Since, “Smith and Jones” has many auction sites, there should be a firewall at every incoming network of each auction site.

### Computer Virus

Computer virus can dangerously infect the computers and hardware devices in an IT system.

**Ways to protect Computer Virus**

**•** Using Antimalware software

* Using Firewall
* Backing Up Data

**Recommendation**

Antimalware software is the most suitable ways for this business. Since each auction site has processing computer devices, antivirus software should be implemented at these devices. Antivirus software can also improve devices’ performance when implemented.

### Employee Theft

Data can also be stolen by unauthorized employee in the business to misuse the data or make malicious functions.

**Ways to protect Employee Theft**

* Using strong password
* Encryption of data
* Controlling with CCTV service

Since **“Smith and Jones”** is a large business with many staffs, controlling business area with CCTV is the best solution for employee theft. Using CCTV service not only protect internal employee theft but also protect the data form external physical attacks.

### Trojan Horse

The attackers try to get access to the IT system by misleading and do malicious activities like deleting data, copying data, etc. (kaspersky, 2020)

**Ways to protect Trojan Horse**

* Anti-spyware software

(Anon., 2019)

* Using Firewall
* Managing Patches

**Recommendation**

Managing patches is suitable for “Smith and Jones” because it enhances the security of software within the business.

### Phishing

Phishing attack can harm the IT system by tricking the staffs with the emails or message and stealing important data.

**Ways to protect Phishing**

* **Using firewall**
* **Using antivirus software**

**Recommendation**

Antivirus software should be implemented at all the devices within the business. Antivirus software not only make the data secure but also prevent the devices form virus.

### Server Failure

Server failure can be caused by loss of power, crashing of operation system, hardware breaks down, etc.

**Ways to protect Server Failure**

* Backing up data
* Using Cloud service
* Keeping power consistent

**Recommendation**

Using Cloud Services is the most suitable method for this business. Using cloud services not only provide data backing up but also ensure safety and security of sensitive data.

### Man in the Middle

Attackers can store the sensitive data or message between customers and business during “Man in the middle” attack.

**Ways to protect Botnet “Man in the middle”**

* Data Encryption
* Using VPN
* Having strong WAP on Access point (Anon., 2020)

**Recommendation**

There should be usage of VPN in every auction site of the business. Since, the VPN create a secure environment within the business, it is the most suitable method for this business.

## Why encryption is necessary

By encryption, the data are encoded so that it cannot be stolen or copied by the unauthorized users. If data are not encrypted, unauthorized persons can easily get access to the data and make malicious processes. (genetec, 2020)

**Encryption for Ecommerce Website**

“Smith and Jones Auctioneers” has an ecommerce website which need encryption. The website should be encrypted by

* **SSL** (Secure Sockets Layer, a technology that help network system safe and secure)
* **TLS** (Transport Layer Security which prevents the website from hackers and unauthorized accesses)

(Annonymous, 2020)

**TLS** is an updated version of **SSL** and it can provide more secure connection. Therefore, TLS should be used in this business.

**Encryption for site to site VPN**

The business auction sites use VPN to connect site to site which require a proper encryption.

**PPTP** provides a secure tunnel for VPN connection and is very easy to setup.

**IPsec** provides flexible method to keep the VPN connection secured and enhance security of IP.

IPsec is more suitable for the business because it works well with most devices and it give highest level of encryption.

**Encryption for Data Store**

There should be an encryption for data storage because it is important to make sure that the sensitive data are safe.

**EFS** - Encryption File System which provides the stored data to be encrypted.

**BitLocker** – works on Windows and encrypts system data and users’ data.

(Thomas, 2013)

EFS should be used in this business because it enhances the security and safety of data stored.

**Encryption for Wi-fi**

Wi-fi connection in auction sites also needs encryption. Wi-fi can be encrypted by

**WPA2,** compliant with IEEE 802.11i standard. WPA2 has two version.

PSK – designed for small businesses and home use.

Enterprise – designed for enterprise networks providing authentication using IEEE 802.1X and EAP.

Since “Smith and Jones” is a large business, WPA2 Enterprise should be used.

**Task - 3**

# Task 3 - Setting up the VPN

## Differences between Intranet and Extranet

|  |  |
| --- | --- |
| Intranet | Extranet |
| * An intranet is a private network that is only accessible by persons in a business. * Basic remote access VPN is extended. * The network connectivity is across the internet. * Manage important information in a single secure location. * Information such as documents, spreadsheets, media files, etc. can be shared through internet. * Use HTTP or other internet protocol to share information of an organization. | * An extranet can be accessible by authorized persons outside the business. * The network is connected by one or more service providers. * It extended the connectivity of network to customers and business partners. * Securely share the information with business partners and customers. * Authorized users are accessible to company’s networks, database and operations. * There should be policies of security to prevent the unauthorized accesses form the outside of business. |

(Anon., 2020)

(Anon., 2020)

### Benefits of Intranet

* **Improve communication within the business**

Intranet enhance the internet communication within the business. It provides teams with open discussions and departmental updates. Anyone within the business can share information.

* **Enhance knowledge Sharing**

Since intranet provides better connection within the business, it is easier for stakeholders to communicate enhancing knowledge sharing.

* **Reduce time**

Using intranet, members of the organization can be easily discuss reducing time cost for meeting and emailing.

* **Improve customer service**

Since staffs can have better access to business information, it enhances the customer service.

(Anon., 2020)

### Benefits of extranet

* **Flexibility**

Using extranet is more convenient to communicate with the persons outside the business such as business partners, clients, etc.

* **Error prevention**

Since extranet provide external communication with customers, it reduces complexity and conflicts between customers and business.

* **Enhance Business relationship**

Since extranet improves external communication, it also enhances the relationship with business partners and customers.

* **Better security to communicate**

The communication and exchanges are under business control and in a secure environment.

(Anon., 2020)

### Recommendation

**“Smith and Jones Auctions”** has to communicate with a lot of customers and business partners. Therefore, using extranet is better option for the business. Moreover, there are online bidding system and payment system which can be securely control by extranet. The web server should be hosted in branch with the use of TLS protocol. IPsec protocol for VPN, EFS for data storage and WPA2 for Wi-Fi should be used in the business network.

## Network Diagram for “Smith and Jones Auctioneers”



(Belisario, 2020)

(Perez, 2019)

## Security features of using VPN firewalls

### Unified Thread Management (UTM)

Firewall provides an efficient account of managing threats in a network. It enhances the security level of the network and sensitive information within a business. (COMODO , 2018)

### Deep Packet Inspection (DPI)

DPI firewall detects the entire flow of network traffic within a business, then filter out harmful attacks and malicious programs. Moreover, DPI can be used for managing network to enhance the network traffic.

(Andress, 2014)

(Rouse, 2017)

### Intrusion Prevention System (IPS)

IPS provides high level security features to a network by blocking unauthorized accesses to the network and malicious programs that can harm the network. In this way, firewall prevent the internal network form the intruders and help sensitive business data secure.

(Firewalls.com Page, 2013)

### Next General Firewall (NGFW)

Next general firewall provides many protection activities for the network. It can provide detection in the network system, specifying IP address with physical locations, blocking dangerous threats and so on (Dooley, 2017)

## Rule of firewall

Access Control List (ACL) – is a firewall rule the enhance the security of the network by blocking unauthorized access. ACL can help to prevent malwares and let users freely bid items. ACL can also block malicious website links which users may unknowingly click. Therefore, ACL provides customers confidence that online bidding process is safe and secure. (Sun Microsystems, 2007)

**Task - 4**

# Task 4 – Maintaining Security

The network security of the business should be maintained by following methods.

## Training

There should be suitable training for staffs and customers to prevent future problems in network. Users should be managed closely with network rules and guidelines.

## Setting Policies for business

There should be network rules and policies of the business which must be followed by staffs and customers.

## Vulnerability assessment

Vulnerability assessments such as network and wireless assessment, Host assessment, penetration testing should be applied to the network system of the business. These testing and assessments can help to identify the security weakness of the network. (imperva.com, 2020)

## Network security Audit

There should be regular reviews for whether staffs and customers follow network rules and polices of the business. The network policies should be managed carefully to business network security. (Dosal, 2018 )

## Contracts and user acceptance check box

Staffs and clients must be provided with user acceptance check boxes. Clients must agree the rules and policies of the business network system.

**Task - 5**

# Task – 5

## Analysis

“Smith and Jones Auctioneers”, world largest auction company, provides online bidding system and wants to keep their network fast and secure. Sensitive data must be protected from malware and virus. Blocking malicious website links is also important. The company wants a web-filtering application in head office. Having 60 auction sites, the company wants to give each auction site own internet connection but the web security for all auction sites want to be control centrally. Moreover, company wants to make sure that guests’ Wi-Fi access is safe and at least 500 clients can connect over Wi-Fi.

## Action Plan

Firstly, the important electronically held information are listed. Some information is got from scenario and some are results from online researches. Then, the possible risks are identified and protection methods for each task are researched online. Being learnt much about encryption and VPN demonstrating protocols is done easily. But drawing network diagram is a bit of work. But it is solved by watching online tutorials. Discussing Firewalls security features is also done easy because of high knowledge about firewall. Methods for maintaining network security are got as knowledge.

## Future Development

There should be more risks in risk identification because there are many other possible risks for a network system. The comparison of intranet and extranet should be more in detail but the word count doesn’t match. Network diagram and case of VPN firewall can say to be successful. Moreover, report writing skill is not satisfying and it should be improved in future.

(NS&C Assignment: Smith and Jones Auctions , 2020 )

# References

Andress, J., 2014. *Deep Packet Inspection Firewall.* [Online]   
Available at: https://www.sciencedirect.com/topics/computer-science/deep-packet-inspection-firewall  
[Accessed 20 June 2020].

Annonymous, 2020. *What is a DDoS Attack?.* [Online]   
Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/#:~:text=A%20distributed%20denial%2Dof%2Dservice%20(DDoS)%20attack%20is,a%20flood%20of%20Internet%20traffic.  
[Accessed 8 June 2020].

Annonymous, 2020. *What is SSL, TLS and HTTPS?.* [Online]   
Available at: https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https  
[Accessed 4 June 2020].

Anon., 2017. *Patch Management can Prevent Security Breaches.* [Online]   
Available at: https://one.comodo.com/blog/patch-management/prevent-security-breaches.php  
[Accessed 1 June 2020].

Anon., 2019. *What is Anti-spyware?.* [Online]   
Available at: https://antivirus.comodo.com/blog/how-to/anti-spyware/#:~:text=As%20its%20name%20suggests%2C%20an,spyware%20cleaner%2C%20and%20spyware%20detector.  
[Accessed 2 June 2020 ].

Anon., 2020. *Benefits of extranet.* [Online]   
Available at: https://www.nibusinessinfo.co.uk/content/benefits-extranet  
[Accessed 7 June 2020].

Anon., 2020. *Benefits of intranet.* [Online]   
Available at: https://www.nibusinessinfo.co.uk/content/benefits-intranet  
[Accessed 7 June 2020].

Anon., 2020. *Difference Between Intranet and Extranet #Intranet vs Extranet.* [Online]   
Available at: https://www.pinterest.com/pin/523684262901330125/?nic\_v1=1a%2ByEpjMMQ7HdlmnozsikUGQ6QwJ0Vqhfq8aix3PJzYWrrNtm5RZNJzh7o%2Fy%2BAfRSN  
[Accessed 6 June 2020].

Anon., 2020. *How Firewalls work.* [Online]   
Available at: https://www.comodo.com/resources/home/how-firewalls-work.php  
[Accessed 23 May 2020].

Anon., 2020. *Intranet vs Extranet.* [Online]   
Available at: https://ungoti.com/blog/intranet-vs-extranet/  
[Accessed 6 June 2020].

Anon., 2020. *Man-in-the-Middle (MITM) Attacks.* [Online]   
Available at: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/  
[Accessed 2 June 2020].

Anon., 2020. *What is a botnet attack?.* [Online]   
Available at: https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp  
[Accessed 20 May 2020].

Anon., 2020. *What is a DMZ Network?.* [Online]   
Available at: https://www.barracuda.com/glossary/dmz-network#:~:text=The%20goal%20of%20a%20DMZ,is%20safe%20behind%20a%20firewall.  
[Accessed 1 June 2020].

Baylor, K., 2018. *The 5 Most Common Website Threats.* [Online]   
Available at: https://allianceitllc.com/5-common-website-threats/  
[Accessed 13 May 2020].

Belisario, D., 2020. *How to Create a Network Diagram.* [Online]   
Available at: https://teams.microsoft.com/\_?culture=en-us&country=WW&lm=deeplink&lmsrc=homePageWeb&cmpid=WebSignIn#/conversations/19:b6dba4da-4645-404b-9ec5-60a7fef08bb4\_d022cd0f-587e-4027-8a08-3783ba2c86d8@unq.gbl.spaces?ctx=chat  
[Accessed 24 June 2020].

COMODO , 2018. *What is UTM Firewall?.* [Online]   
Available at: https://cdome.comodo.com/blog/what-is-utm-firewall/  
[Accessed 11 June 2020].

Dooley, K., 2017. *What to Look for in a Next-Generation Firewall.* [Online]   
Available at: https://www.auvik.com/franklymsp/blog/next-generation-firewall/  
[Accessed 20 June 2020].

Dosal, E., 2018 . *How a Network Security Audit Works & Why It’s Important.* [Online]   
Available at: https://www.compuquip.com/blog/how-a-network-security-audit-works-why-its-important#:~:text=The%20network%20security%20audit%20is,risk%20of%20a%20security%20breach.  
[Accessed 21 June 2020].

Firewalls.com Page, 2013. *How Intrusion Prevention Systems (IPS) Work in Firewall?.* [Online]   
Available at: https://community.spiceworks.com/topic/362007-how-intrusion-prevention-systems-ips-work-in-firewall  
[Accessed 20 June 2020].

genetec, 2020. *What is encryption and how important is it?.* [Online]   
Available at: https://resources.genetec.com/blog/what-is-encryption-and-how-important-is-it#:~:text=Encryption%20is%20the%20process%20through,between%20client%20apps%20and%20servers.  
[Accessed 3 June 2020].

imperva.com, 2020. *Vulnerability assessment.* [Online]   
Available at: https://www.imperva.com/learn/application-security/vulnerability-assessment/  
[Accessed 21 June 2020].

kaspersky, 2020. *What is a Trojan Virus.* [Online]   
Available at: https://www.kaspersky.com/resource-center/threats/trojans  
[Accessed 2 June 2020].

Melnick, J., 2018. *Top 10 Most Common Types of Cyber Attacks.* [Online]   
Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/  
[Accessed 13 May 2020].

*NS&C Assignment: Smith and Jones Auctions* (2020 ) NCC Education .

Perez, M., 2019. *Tips for mapping your network diagram.* [Online]   
Available at: https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/tips-for-mapping-your-network-diagram#:~:text=A%20logical%20network%20diagram%20illustrates,traffic%20flow%20and%20network%20segments.  
[Accessed 24 June 2020].

Rouse, M., 2017. *antimalware (anti-malware).* [Online]   
Available at: https://searchsecurity.techtarget.com/definition/antimalware  
[Accessed 23 May 2020].

Rouse, M., 2017. *deep packet inspection (DPI).* [Online]   
Available at: https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI  
[Accessed 20 June 2020].

Spacey, J., 2017. *15 Examples of Information asset.* [Online]   
Available at: https://simplicable.com/new/information-asset  
[Accessed 13 May 2020].

Sun Microsystems, 2007. *Configuring Access Control Lists (ACLs).* [Online]   
Available at: https://docs.oracle.com/cd/E19859-01/820-3252-11/FP44ucgACL.html  
[Accessed 21 June 2020].

Thomas, G., 2013. *What are differences between EFS and BitLocker in Windows?.* [Online]   
Available at: https://superuser.com/questions/527010/what-are-differences-between-efs-and-bitlocker-in-windows#:~:text=BitLocker%20encrypts%20all%20personal%20and,individual%20files%20on%20any%20drive.  
[Accessed 5 June 2020].

# 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 acknowledge 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?

