Set Task Electronic Template – Unit 11

Task A - Activity 1 Template: Risk assessment of the networked system

Risk severity matrix

Probability of threat occurring	Very likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
	Size of the loss			

Assessment

Number	Where Threat found	Threat type	Threat
1.	Guest Wi-Fi and mobile devices	Implied	Misconfigured Nat on router could allow unrestricted access to guests.
2.	Wi-Fi router with optical fibre and CAT6 connections	Specific	Optical fibre cables and cat6 cable too close together will disrupt data transmission.
3.	Servers	Implied	Open ports unblocked. This leaves the servers vulnerable to port scanners who could identify open ports and access the servers through them.
4.	Staff PC's	Implied	Key logging could allow a hacker to follow every input which the staff may have made on the computer allowing them fraudulent access to valuable

			information.
5.	**Staff Wi-Fi and mobile devices**	**Implied**	**Misconfigured SSID or encryption on Wi-Fi. Any user could access the same Wi-Fi point as the staff if the SSID is misconfigured. This could lead to unpermitted access to data.**
6.	**Servers**	**generic**	**Port scanners could be used from the restaurant and coffee bar on the 20th floor to scan for open ports in the servers.**
7.	**Staff PC's**	**Implied**	**Misconfigured firewalls could allow easy access for hackers to access company data.**
8.	**Server**	**specific**	**Admin server must not be visible**
9.	**Wi-Fi router with optical fibre and CAT6 connections**	**specific**	**Wi-Fi must not connect to IOT devices.**
10.	**Guest WAP**	**specific**	**Open RJ45 ports can be used to access the servers.**
11.	**Guest Wi-Fi and mobile devices**	**generic**	**Internet likely to be attacked**
12.	**Electronic door control system**	**generic**	**Likely to be attacked**

Threat number.	1
Risk severity.	High
Threat title.	Unrestricted access of guest Wi-Fi and mobile devices
Probability.	Likely
Potential size of loss / impact level.	Moderate
Explanation of the threat in context.	If guests have an unrestricted level of access there are no policies in place which will prevent them from accessing and stealing tempering with valuable company data.

Threat number.	2
Risk severity.	Low
Threat title.	Mixed data and electrical cabling effecting data transmission
Probability.	likely
Potential size of loss / impact level.	Minor
Explanation of the threat in context.	When the optical fibre cable and CAT6 connection cables are to close by to each other it could cause a data transmission failure which could lead to staff and company data being lost.

Threat number.	3
Risk severity.	Extreme
Threat title.	Unblocked open server ports
Probability.	Likely
Potential size of loss / impact level.	Major
Explanation of the threat in context.	If the server happens to have any open ports which should always be blocked, hackers may be able to use port scanners to identify open ports and hack them. They will then have access to confidential data such as trade secrets.

Threat number.	4
Risk severity.	High
Threat title.	Keylogging of Staff PC's
Probability.	Unlikely
Potential size of loss / impact level.	Major
Explanation of the threat in context.	Hackers may use a program which allows them to key tag every key that a member of staff enters into their PC's such as usernames and passwords. In this case it is dangerous as it could be used to access and modify confidential company data.

Threat number.	5
Risk severity.	medium
Threat title.	Misconfigured SSID or encryption on Staff Wi-Fi
Probability.	Likely
Potential size of loss / impact level.	Moderate
Explanation of the threat in context.	A misconfigured SSID or encryption in this network on the staff Wi-Fi would mean that any user could access the same Wi-Fi point as the staff if the SSID is misconfigured. This could lead to unpermitted confidential access to data.

Threat number.	6
Risk severity.	Extreme
Threat title.	Port scanners used from restaurant and bar on 20th floor
Probability.	Low
Potential size of loss / impact level.	Major
Explanation of the threat in context.	Guests on the 20th floor using the restaurant or bar may attempt to use port scanners in order to find open ports ion the servers. This is extremely dangerous as if open ports are located, hackers can access unlimited confidential information.

Threat number.	7

Risk severity.	High
Threat title.	Misconfigured firewalls on staff PC’s
Probability.	Likely
Potential size of loss / impact level.	Moderate
Explanation of the threat in context.	If a Staff PC has a misconfigured firewall this leaves it vulnerable to hackers in this scenario. Unfortunately this could prompt unwanted access to confidential data within the PC and the servers.

Threat number.	8
Risk severity.	Low
Threat title.	Visible admin server
Probability.	Very likely
Potential size of loss / impact level.	Minor
Explanation of the threat in context.	If guests or hackers are able to locate the admin server this could be dangerous as they could hack their way into a Staff’s account and access their data. They shouldn’t create a VLAN in this scenario in order to ensure a secure logical segmentation of networks

Threat number.	9
Risk severity.	High
Threat title.	Wi-Fi routers connection to IOT
Probability.	Very likely
Potential size of loss / impact level.	Minor
Explanation of the threat in context.	A connection to IOT is very dangerous for this company in this scenario as it allows easier access for hackers connecting to the internet to steal confidential data.