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			

financial, reputational, operational, legal

Assessment

Threat number.	1
Threat title.	Attacks via the Wi-Fi
Probability.	Very Likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	Hackers may use automated scanning software to find ways to gain unauthorised access to the network. This is dangerous as the Wi-Fi can be connected by mobile devices. This will lead to financial, reputational and operational loss for BCTAA.

Threat number.	2
Threat title.	Attacks via remote access
Probability.	Very Likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	Hackers may use automated scanning software to find vaulenables in the network allowing them to gain unauthorised access to the network. Other ways attacks can access is by eavesdropping on the remote access user to gain their secrets. This will lead to financial, reputational and operational loss for BCTAA.

Threat number.	3

Threat title.	Attack on clients information
Probability.	Very Likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	With the company BCTAA being in contact with their clients highly confidential information they need to be careful as a Hacker can use scanners to check for valunables on the network and steal the client's confidential information. This will lead to financial, legal and reputational loss for BCTAA.

Threat number.	4
Threat title.	Misconfigured patch panel- Main switch
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	An attacker can swap the Cat6 cable for another cable and gain direct unauthorised access to the network and will be able to have full control of the network. This will lead to financial, reputational, operational and legal loss for BCTAA.

Threat number.	5
Threat title.	Misconfigured Firewall
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	If the Firewall is not configured and maintained correctly the firewall will allow potentially dangerous packets to enter the network and could lead to an overload in the network and it crashing. This will lead to financial, reputational and legal loss for BCTAA.

Threat number.	6
Threat title.	Misconfigured controlled doors
Probability.	Likely
Potential size of loss / impact level.	Major

Risk severity.	High
Explanation of the threat in context.	As the management of the office building provide the key cards and the software to run the controlled door, the admin officer may not keep updated on maintaining the door, another possibility is that members of the public or other companies may act as an employee of BCTAA to get a key card to gain unauthorised access. This will lead to reputational and legal loss for BCTAA.

Threat number.	7
Threat title.	Misconfigured access rights
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	If a client or visitor to the office uses the internet they could possible using a staff account that has access to client's confidential information, if this information gets into the wrong hands it may cause the network problems or they might steal the confidential information. This will lead to financial, reputational, operational and legal loss for BCTAA.

Threat number.	8
Threat title.	Misconfigured or weak password policy
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	A weak and misconfigured password policy can leave the company at risk of losing their clients data by having a weak password and/or it not being regularly updated and changed. Current BCTAA don't have a password policy for their staff which leaves the clients confidential information at risk. This will lead to financial, reputational, operational and legal loss for BCTAA.

Threat number.	9
Threat title.	Attack by breaking and entering
Probability.	Unlikely
Potential size of loss / impact level.	Major
Risk severity.	Medium
Explanation of the	As there is a bars and restaurants above the office and is accessible by

threat in context.	walking past the BCTAA office when they are closed this may cause a security risk and an unauthorised user may break into the office and vandalise or steal information for the office. This will lead to financial, reputational and operational loss for BCTAA.

Threat number.	10
Threat title.	Misconfigured SSIDS or encryption of Wi-Fi
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	When the Wi-Fi is first set up it has a default password which is strong and hard to remember. This can lead to a hacker guessing the password as it is default and has not been changed they have a higher chance to gain access and change the password and cause confusion within the company. This will lead to financial, reputational and operational loss for BCTAA.

Threat number.	11
Threat title.	Attack on unused open ports
Probability.	Very Likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	An Attack can use an automated port scanner to locate of there is any unused open port with the network they can then send packets onto the network causing it to become overrun and fail or gain access to the network via the unused open port. This will lead to financial, reputational and operational loss for BCTAA.

Threat number.	12
Threat title.	Leaking of clients information by unhappy staff member
Probability.	Unlikely
Potential size of loss / impact level.	Major
Risk severity.	Medium
Explanation of the threat in context.	If an employee becomes unhappy or upset at the company or a client, they may leak their clients or BCTAA confidential information to the public or the press.

	This will lead to financial, reputational, operational and legal loss for BCTAA.

Threat number.	13
Threat title.	Misconfigured NAT
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	Without a configured NAT, it is setup as default. This may cause a problem by not connecting them together causing problem within the network and making an attackers job easier to gain access to the network. This will lead to financial, reputational and operational loss for BCTAA.

Threat number.	14
Threat title.	Weak encryption in VPN
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	If the company uses a weak and unsecure method of encryption VPN for remote access to their client's confidential information this may lead to a higher risk of the client's secrets being stolen due to a man in the middle attack this could lead to major legal, financial and reputational loss.

Threat number.	15
Threat title.	Attack via mobile devices
Probability.	Very likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	Hackers may use automated scanning software to find ways to gain unauthorised access to the network via the Wi-Fi. This is dangerous as the Wi-Fi can be connected by mobile devices which is portable and can be accessing the Wi-Fi from anywhere in the building. This will lead to financial and reputational loss for BCTAA

Threat number.	16
Threat title.	Attack via visible servers on the Wi-Fi network
Probability.	Very likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	When the list of possible Wi-Fi connection the BCTAA servers come up available for connection, this can allow hackers to use automated scanning software to find ways to gain unauthorised access to the network. This is dangerous as the Wi-Fi can be connected by mobile devices which allows the hacker to be anywhere in the building. This will lead to financial and reputational loss for BCTAA

Threat number.	
Threat title.	
Probability.	
Potential size of loss / impact level.	
Risk severity.	
Explanation of the threat in context.	