Introduction: Network security is the important part of every organization to protect data and different types of network attacks. Café Italia is a coffee shop which they want to upgrade their network security and old system. The CEO called me as a consultant for help to secure their business and provide safe Wi-Fi networking for customers.

Task 1 – Risk Assessment

a) Important electronically held information assets relating to *Café Italia*:

1. Employee personal data.
2. Customer's data.
3. Order processing.
4. Financial data.
5. Email data.

b), c), d) the list of assets with the security threats and their security risk:

Asset	Threat	CIA?	Likelihood	Impact	Risk
Employee personal data	Server failure	A	Low	Medium	Low
	Theft	C	Low	Medium	Medium
	Spyware	C	Low	Medium	Medium
Customer's data	Virus	A	Low	Medium	Low
	Server failure	A	Low	Medium	Low
	Employee theft	C	Low	High	Medium
	Phishing	C	Medium	High	High
Order processing	Trojan horse	I	High	Medium	High
	SQL injection	I	Medium	High	Medium
	Malware	A	High	Low	Medium
	Ransom ware attack	A	Medium	High	High
	Spyware	C	Medium	High	Medium
Financial data	Malware	I	Low	Medium	Medium
	Ransom ware attack	A	High	High	Very high
	SQL injection	I	Low	High	Medium
	Spyware	C	Medium	Medium	Medium

	DDoS	A	Medium	High	Medium
Email data	Ransom ware attack	A	High	High	Very high
	Phishing	C	Medium	Medium	Medium
	Virus	A	Medium	High	High
	Sarver failure	A	Low	High	Medium

Task 2 – Explaining Risk Control

a) After analyzing the scenario of Café Italia, it's clear that they need to be increased their network security. I have identified security threats of network and possible solutions are given below:

Data at rest (Server):

Data at rest when it is stored on server. Café Italia keeps their data at their own server and which is configured as a domain controller running Windows Server 2008 R2. They store their all data include financial systems, order processing, email and human resources (employee) data and IT. Many internal and external attacks can be happened on the server. The denial of service (DOS) attack is one of the most powerful and dangerous cyber-attacks. And also Injection Attacks, Brute Force can lose of server data and hacked by someone. R2 server and email server are protected and being secure using DMZ protection (Anon., n.d.).

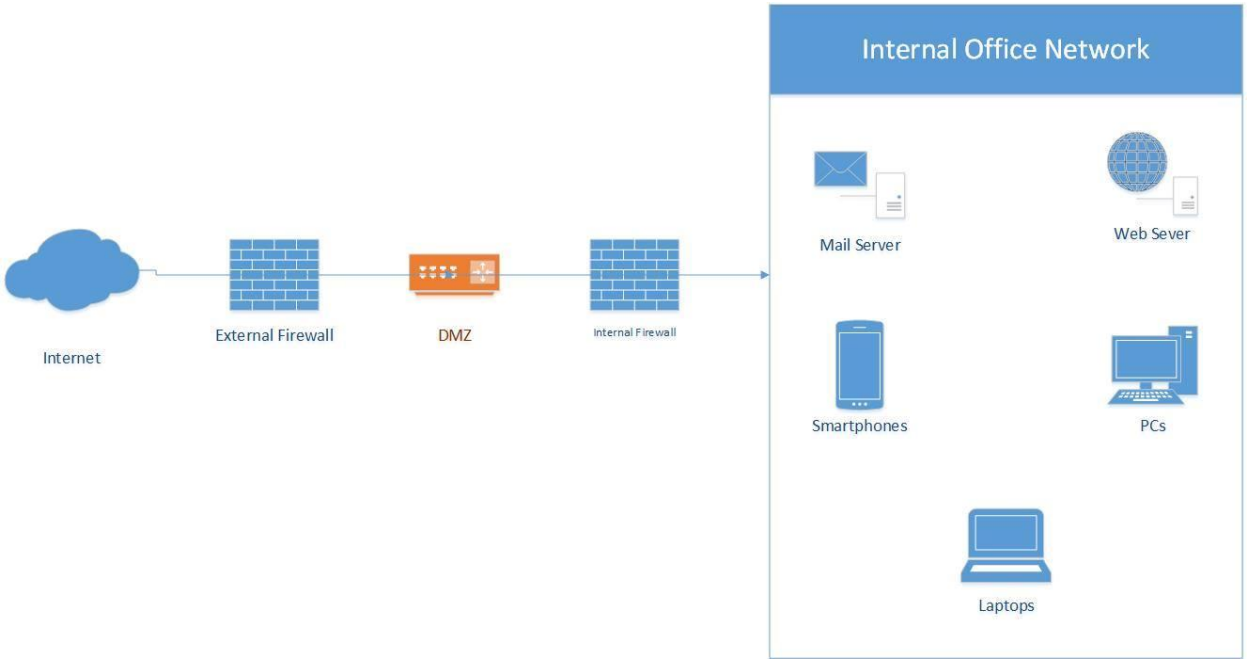

Figure 1: DMZ protecting servers from internal and external attack.

It is needed to be followed the below steps properly protected if the server data is stored.

Solution:

- Email server and R2 server are needed to be placed in DMZ.
- Default configuration cannot be selected.
- Ensure secure configuration.
- Unnecessary service port must be off.
- Restriction of removal media.
- Properly update and patch management.
- Monitoring the server in a regular basis.
- To make server reliable backup should be ensured.
-
- Keep UPS for uninterrupted power supply.
- Keep system backup.

Data security:

It is needed to introduce a new security policy for Café Italia to make secure the metadata. System financial data, Order processing data, IT, Email and Human resources data should provide protection.

Solution:

- Creation of user group.
- Creation of files and folders.
- Encrypt the important file and folders.
- Implement company information security policy.
- Implement standard password policy.
- Implement access authentication system.
- Keep access control lists.
- Restriction of unauthorized download.
- Cloud data storage backup is needed.

Data at transmission:

Making a secured pathway between head office to branch offices. They use Cat-5 LAN cable to make connection between head office and branch offices and EPOS system is also available in each branch. So it is most important to provide security in this way of transmission. Phishing attack and Trojans attack can be happened while data transmission (Anon., n.d.).

Solution:

- Deploying VPN to head office and branch offices connections.
- Restriction on unauthorized download.
- Encryption policy can be deployed to make data transmission secured.
- To make the system highly secured Digital signature should be used.

Remote access:

Providing remote access facility to its customer, business staff and employees, there is a responsive website. Data get transferred from website to the data user. So it is badly needed to provide security on this transmission. DoS attacks, DNS Poisoning, Port scanning, TCP DE synchronization, SMB Relay, ICMP attacks are common threats while remote access (Anon., n.d.).

Solution:

- Keep open VPN.
- Deploying secured application.
- Dialup massage while remote access should be encrypted.
- Security policy should be invoked while configuration.

Network hardware security:

Hardwar components are the tangible equipment of network. Network components like Access pointer, PCs, Printer, Graphical eyes, Firewall are under risk of thermal heat and natural theft.

Solution:

- Introducing physical access control system.
- Physical security of hardware components.
- Keep backup of all hardware components.
- Room temperature should be controlled.
- Proper maintenance of hardware components.
- Get prepared to face natural disasters.

b) Cyber security helps to focus on business objectives and protected cyber-attacks. The 10 steps of cyber security are given below:

10 steps to Cyber Security:

1. Risk management regime.
2. Secure configuration.
3. Network security.
4. Managing user privileges.
5. User education and awareness.
6. Incident management.
7. Malware prevention.
8. Monitoring.
9. Removable media controls.
10. Home and mobile working (Anon., n.d.).

The ISO 27001 Information security management system is the international best practice standard for information security. The 10 steps of ISO27001 are given below:

10 steps to ISO27001:

1. Decision.
2. ISO Management Representative.
3. Gap Analysis and Risk Assessment.
4. Scope & Implementation Plan.
5. Employee Introduction.
6. Documentation, documentation, documentation!
7. Realization.
8. Internal ISO 27001 Audits.
9. ISO 27001 Certification.
10. Maintaining the ISO 27001 Certification (Anon., 2017).

c) Yes, we have placed our important two servers including email server and R2 server into DMZ switch. Server get protected internally and externally using DMZ. File and folders are encrypted and data security is also given in the server. Encryption has done using AES algorithm and EFS feature of windows. Also, Triple DES, RSA, Blowfish and Two fish are common algorithms while data encrypted. Data transmission form head office to branch offices through VPN. And IPsec, Point to Point Protocol, Signal Protocol and Transport Layer Security are common protocol while data encrypted (Anon., n.d.).

Task 3 – Network Diagram

a) The proposed network diagram of Café Italia:

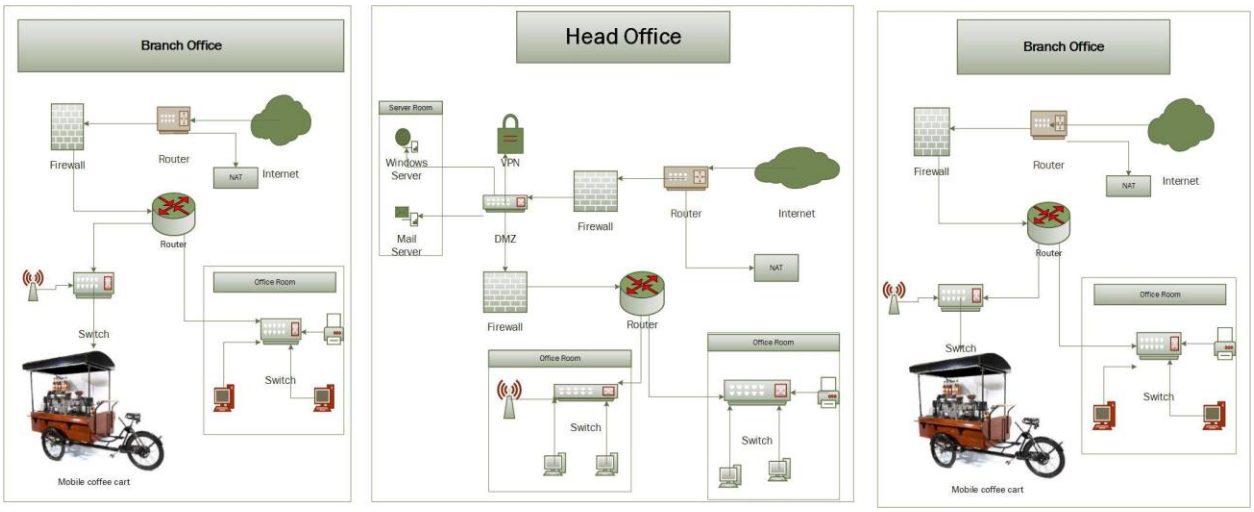

Figure 2: Proposed network diagram of Café Italia.

b) The proposed network diagram of Café Italia with realistic IP address:

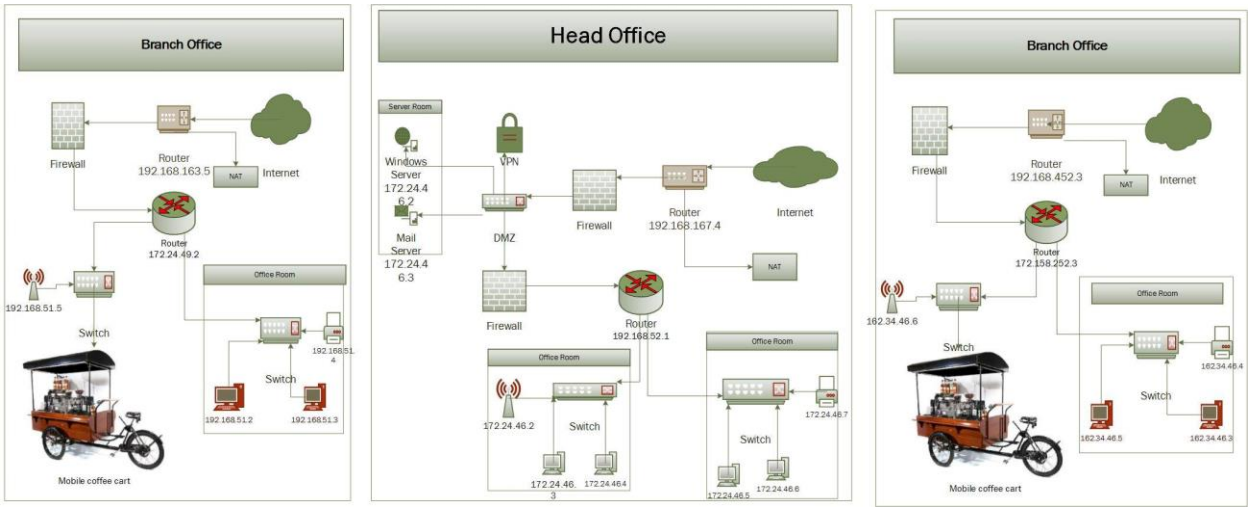

Figure 3: Proposed network diagram of Café Italia with realistic IP address.

c) In task 1 and task 2, I have designed the network diagram with realistic IP address for Café Italia. In both of the task I am showing how to protect their network security and protect their data. I am also using all of the network components for better security. So, the simply describe of network components are given below:

- The servers like R2 server and email server, where stored the all data including financial system, order processing, IT, email and human resources data. As a result of using DMZ, he stored data can be protected from internal and external attacks.
- VPN can establish securely transmission in head office to branch offices and create a secure tunnel.
- The files and folders are stored as an encrypted file using AES algorithm and EFS feature of windows.
- Firewall can be created proper security configuration in the network. It can be secured data from unauthorized access.

I tried my best to secure the network as possible. So if all the security systems maintain proper way, the network security of Café Italia will be safe.

Alternative solutions:

- To make the system highly secured Digital signature should be used.
- To make server reliable backup should be ensured.
- Dialup massage while remote access should be encrypted.
- Cloud data storage backup is needed.
- Get prepared to face natural disasters.

Task 4 – Customer Wi-Fi

Analyzing the scenario Café Italia, it is seen that their website is so vulnerable. The thefts and the solutions are identified and recommendation are provided. So future maintenances which are needed explain below:

- It is bolded that Café Italia's main security concern is about Wi-Fi service. Wi-Fi honey pot is known as Wi-Fi honey AP and it is an effective rogue to snatch data (Anon., n.d.).
- Secure interface provide by using firewall, DMZ and VPN technology.
- Standard security policies have to be implemented to ensure Café Italia security including restriction downloading and restriction of using removable disk.
- To maintain the security properly it is must to encrypt the file, backup the file and maintain access of authorization.
- Identify threats and prevent them monitoring the server and hardware regularly.
- Network monitoring to ensure is unnecessary computer connect to network.
- Unnecessary service port must be off thus opportunity of unauthorized access can be reduced.

Task 5 – Reflective commentary

a) I faced the problem that to complete the all task is the restriction of time. It's not enough time for me to complete the whole task of scenario properly in this short time. If I had more time for analyze the scenario, I hope there was more security in the system.

b) If I could start again, I would spend more time analyze the whole task of scenario. I would like to add more threats and solutions in the network security. And also I would like to add more diagram and security information in the all task.

Conclusion: After analyzing the current system of Café Italia, to ensure the network security VPN has been provided secure data transmission. And DMZ has been placed in the server for external and internal threats. So if all the security systems maintain proper way, the network security of Café Italia will be safe.

References

Anon., 2017. [Online]
Available at: https://www.theagenci.com/iso27001/10-simple-steps-to-iso-27001-certification-html/

Anon., n.d. [Online]
Available at: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
[Accessed 26 April 2017].

Anon., n.d. [Online]
Available at: https://www.storagecraft.com/blog/5-common-encryption-algorithms/
[Accessed 26 April 2017].

Anon., n.d. [Online]
Available at: https://www.wifipineapple.com/
[Accessed 26 April 2017].

Anon., n.d. [Online]
Available at: http://support.eset.com/kb2907/?locale=en_US
[Accessed 26 April 2017].

Anon., n.d. [Online]
Available at: https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest
[Accessed 26 April 2017].

Anon., n.d. [Online]
Available at: http://searchsecurity.techtarget.com/tip/Secure-data-transmission-methods
[Accessed 26 April 2017].