Acknowledgement

First of all, I am expressing my thanks to almighty for his special kindness to give me the opportunity to complete the assignment successfully. Then I would like to thank our course instructor for his continuous support, supervisor, suggestion and providing me with valuable information that was very much needed for the completion of this presentation.

Introduction:

iSee clinic is an eye hospital which has faced ransomware attack very recently. From this scenario the company asked me as the network consultant to identify the security issues and threats and provide better solution for ensuring the safe and secured network for them.

Task1

a) Five important electronically held information assets relating to isee clinic are following:

I. Patient personal data
II. Order processing
III. Financial data
IV. Employee data
V. Specialist equipment data

b), c), d):

The list of assets with the main security threats and their impacts on the company are explained here.

Asset	**Threat**	**CIA?**	**Likelihood**	**Impact**	**Risk**
Patient personal data	Server failure	A	low	medium	Low
	Employee theft	C	low	high	Medium
	Phishing	C	medium	high	High
	Malware	I	medium	medium	Medium
Order processing	SQL injection	I	medium	high	High
	Buffer overflow	A	low	high	Medium
	Trojan horse	I	high	high	High
	Eaves dropping	C	medium	high	High
	Phishing	C	medium	medium	Medium

Financial data	Financial malware	I	high	low	Medium
	Malicious spyware	C	medium	medium	Medium
	SQL injection	I	medium	high	High
Employee data	Theft	C	low	high	Medium
	Server failure	A	low	medium	Low
	Eaves dropping	C	low	medium	Low
	Spyware	A	medium	medium	Medium
Specialist equipment data	Spyware	C	high	High	High
	Server failure	A	low	medium	Low
	Phishing	C	medium	high	High

Task2

a) Recommended security solutions:

It is seen that iSee clinic is an eye hospital which is recently faced ransomware attack and it encrypts much of the data on their network. It stopped all services and the clinic not being able to operate for a week. Finally, the company is bound to give ransom to run the system. It causes a large amount and company's reputation to be lost. So it is must to build a secure network for this company now to prevent that type of all attacks. For this, the risks of iSee clinic network are identified and the solutions are also recommended here.

Risk 1

Server (data at rest)

The most two important servers- **domain controller server** where all important data like patient data, financial data, employee data and transaction data are stored and **email server** which is used for communication are so much vulnerable than other servers. For this reason, it has faced ransomware attacks very recently. Besides, it mostly faces malware attacks. Many internal and external attacks like bruteforce attack, Dos attack create problems also. So if server is not protected properly, these data may be lost or hacked by someone.

Solution:

- Place the server in DMZ (demilitarized zone) to protect it from internal and external threats because it creates a secured zone on each side of a firewall by following process:
  Internet connected to firewall via router. Again workstations and other servers are connected to firewall via router on opposite side. So, there are two firewalls and DMZ is established between them. So it is now a secure

zone and if the server where valuable data is stored is placed here, it will be protected by external threats which can come through internet and internal threats which can come from workstations.

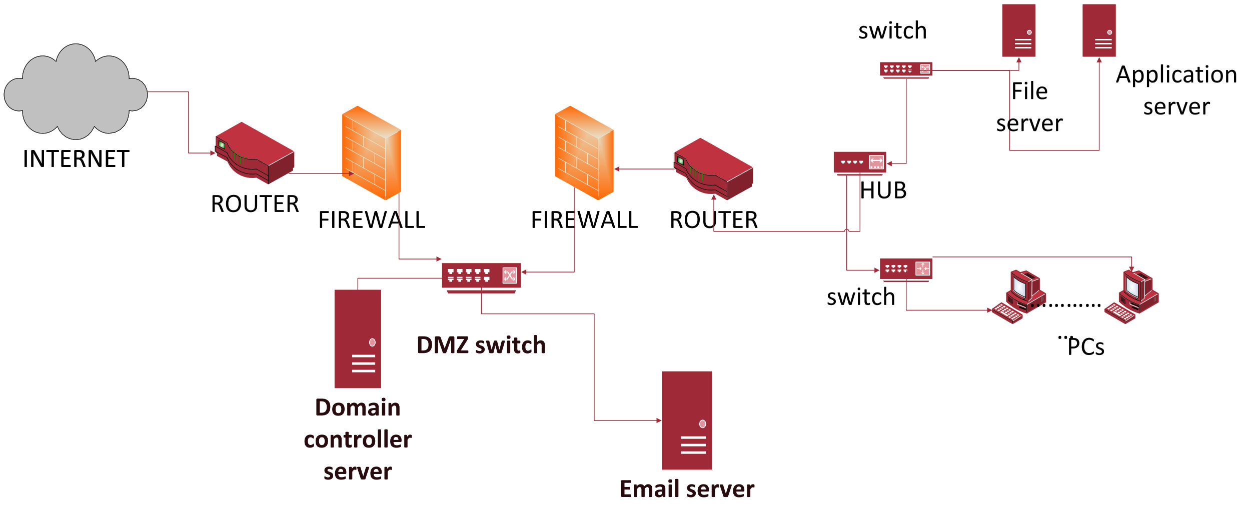

Figure 1: domain controller and email servers are deployed in DMZ zone.

- Default configuration should be avoided and secure configuration should be applied.
- Latest security patches should be installed.
- Unnecessary service port should not be opened.
- Two step authentications should be established.
- Regular security auditing.
- Maintain the best practices.
- Data should be back up regularly in cloud.
- Monitor server room for preventing theft.

Risk 2

Data in transmission:

Data have a risk of phishing, Trojan, spyware, malware attack while it is transmitting. So protection should be established for secure transmission of data.

Solution:

- Firstly, VPN(virtual private network) should be deployed with head office and branch offices because it allows authorized users to pass data through the firewalls and ensures integrity and confidentiality. It does this by creating a private communication tunnel between headquarter and branch office by using **IPSec**, **PPTP** and **L2TP** protocols.

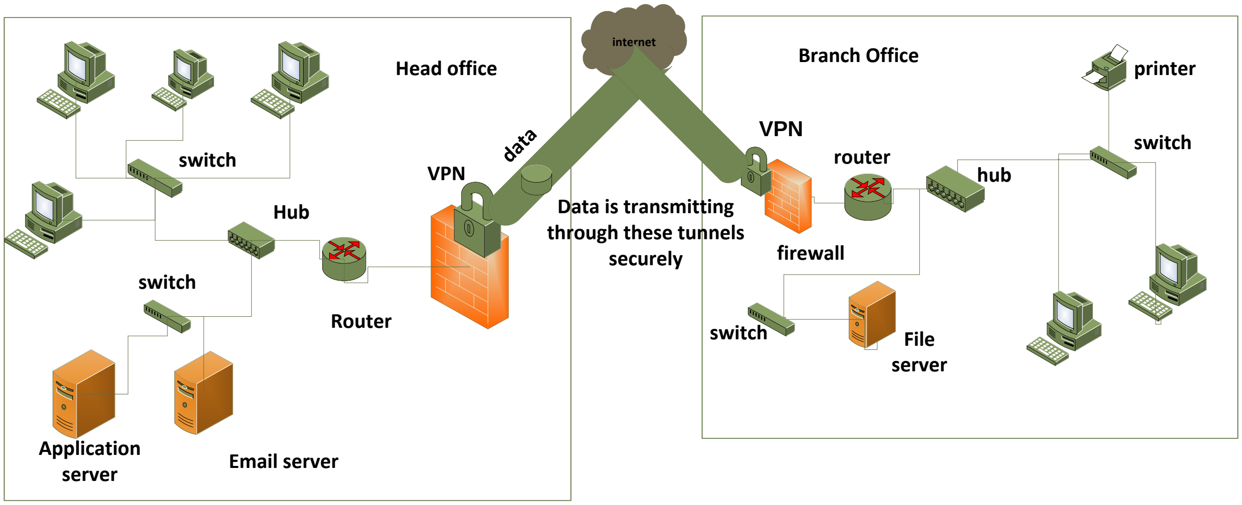

Figure 2: VPN creates a secure tunnel for providing data transmission security

- SSLVPN should be used to encrypt data while transmitting.
- Anti-phishing protection and anti-malware application should be deployed.
- Digital signatures should be used.

Risk 3

Hardware:

Hardware's are tangible things and most of time they can be damage by physical or natural process such as heating, any type of physical force, power voltage surges (datarecoverylabs.com). So it should be protected properly.

Solution:

- Using Stabilizer and making sure no electrical discharge happened while operating.
- A surge protector and uninterruptable power supply should be considered.
- Installing security camera for monitoring.
- An alarm should be attached that will sound if any equipment is displaced.

Risk 4

Data security

Data that is stored in a folder or as a file also have a risk of confidentiality, integrity and availability because of malware attacks, unauthorized access and theft. So it should be protected properly.

Solution:

- Access control mechanism should be used to set permissions for folders and individual files.
- Full disk encryption should be used to encrypt the whole disk.
- Cryptographic file system should be used to encrypt all data including metadata.

- Software applications should be installed which allow user to password protect individual documents.
- Data should be back up in cloud or another server.

Risk 5

Remote access:

As this network will be accessed remotely by the users, security issues of this network must be strong enough to resist the incoming threats.

Solution:

- Using RDP gateway which provides a way to restrict access to remote desktop ports while supporting remote connections (security.berkeley.edu).
- OpenVPN should be used which provides secure connection in remote access.
- Setting up account lock up policy.
- Using encryption to secure dial up remote access connection (techgenix.com)
- Deploying secure applications.

b) 10 steps of cyber security:

Cyber security defines technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access (advisera.com). The 10 steps of cyber Security are following:

- **Risk management regime**

  Defining Risk management regime is central in an organization overall cyber security strategy.

- **Secure configuration**

  Security patches should be applied to ensure the maintenance of secure configuration of all ICT systems.

- **Network security**

  Network should be protected against external and internal attacks by managing network perimeter and filtering out unauthorized access and malicious content.

- **Managing user privileges**

  Account management processes should be established and the number of account privileges should be limited (gov.uk).

- **User education and awareness**

  User security policies, staff training should be established and user awareness of cyber risk should be maintained.

- **Incident management**

  Incident response and disaster response capability should be established.

- **Monitoring**

  Monitoring strategy and supporting policies should be produced.

- **Removable media controls**
  A control should be produced to control all access to removable media.

- **Home and mobile working**
  A mobile working policy should be developed.

- **Malware protection**
  Anti malware should be established.

ISO 27001:

By above mentioned definition, it can be said that cyber security is procedures and applying technology in a secure way. ISO 27001 is an international standard that defines how to manage these tasks to protect digital assets and it helps a person by following ways regarding cyber security:

- It customizes the protection of information system and focuses on particular issues of an organization as its philosophy based on risk assessment.
- It focuses on how to manage the relationship between organization, people and technology.

c) Recommended protocol and encryption algorithm:

Following protocols and encryption algorithms are required where encryption is used:

- **for authentication:**

  IPSec protocol, AES and RSA algorithm are used to provide authentication. Also hashing algorithm may be used for password protection.

- **For establishing VPN:**

  IPSec (IP security), PPTP (point-to point tunneling protocol), L2TP(layer 2 tunneling protocol) are used to create the VPN tunnel. Public key encryption techniques and AES algorithm are used to encrypt data that moves through this tunnel.

- **For data storage:**

  Symmetric encryption is used to encrypt data at rest and AES algorithm is used for file folder encryption.

Task3

a) Network diagram of the company:

This diagram shows the whole network of the company using the network components.

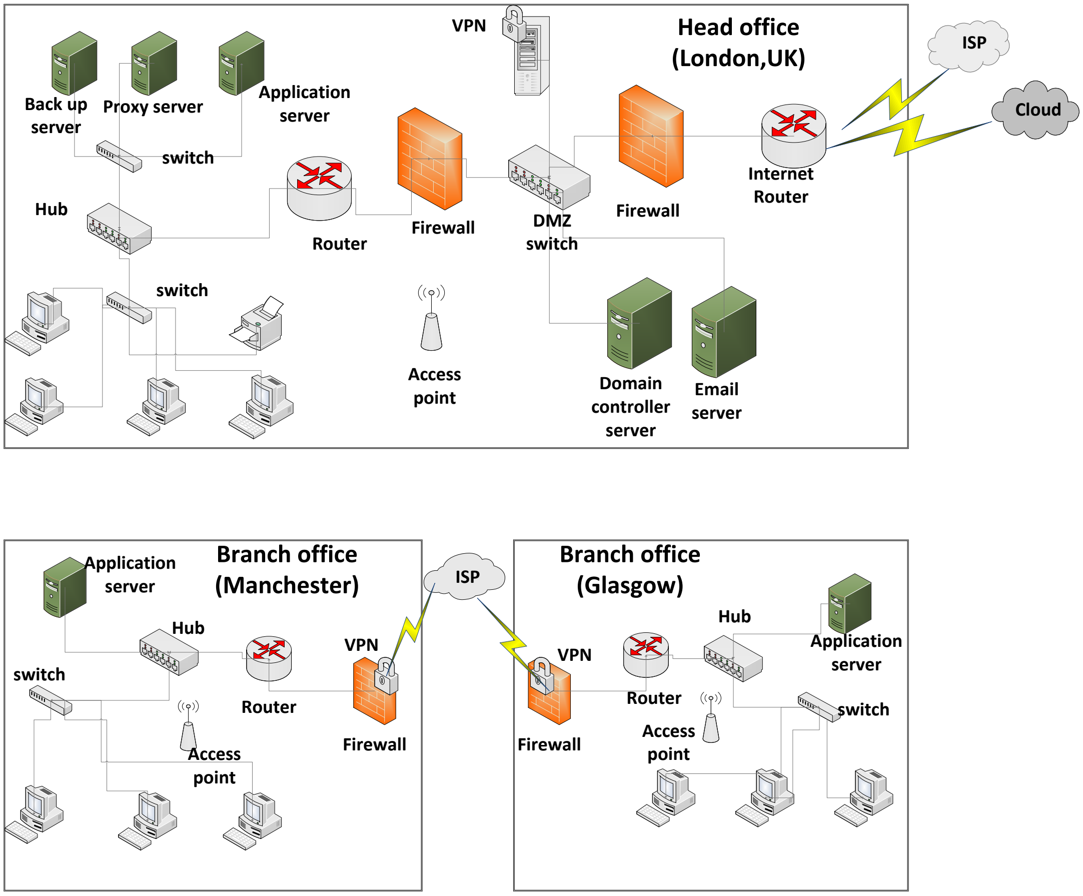

Figure 3: network diagram of iSee clinic.

b) Network diagram of the company including IP addresses.

This diagram shows the whole network of the company using the network components with IP addresses.

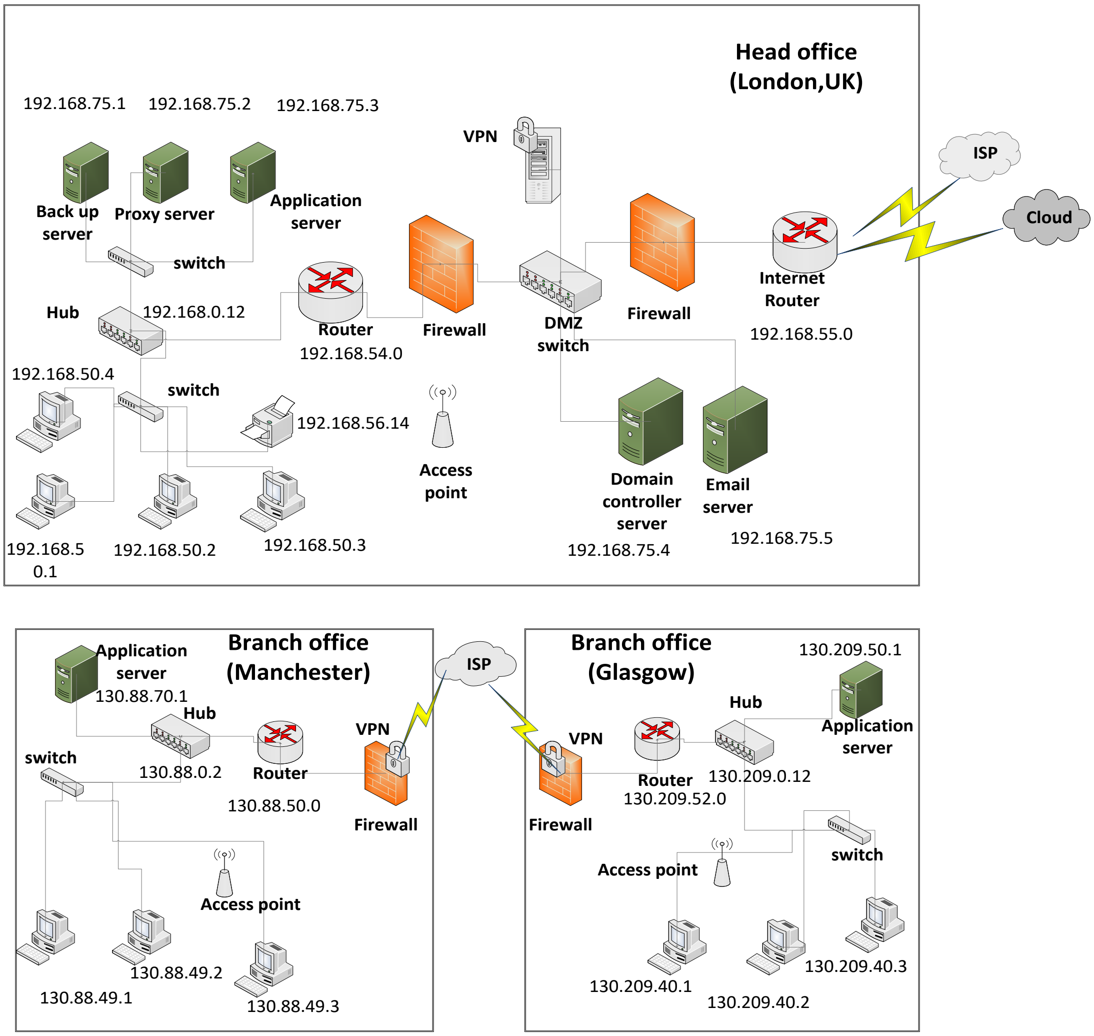

Figure 4: network diagram of iSee clinic with IP addresses.

c) Evidence of meeting security requirements:

In task 1 and task2, important electronically held information assets relating to iSee clinic have been identified and the highest risks of this system and also their protection have been explained. From above explanation some security requirements are noticed that are following:

- The servers (**domain controller and email server**) where valuable data like patient and employee data, financial data are recorded are so much vulnerable rather than other servers. If it is placed in **DMZ zone** the stored data can be protected from external and internal threats. **(referred to figure1)**
- **VPN** is established in branch office and head quarter so that it will create a secure tunnel and data is **transmitted securely** into it. **(referred to figure)**
- Data which are stored as **file or folder** in a system are encrypted using **file encryption system** so that data can be secured from unauthorized access and malwares.

Alternative solutions:

- **Proxy server** which acts as an intermediary between client and server should be established to prevent direct connection between them. It provides **anonymous browsing and filters request** from external site.
- Data should be **back up** in cloud. So, it can be found if necessary.
- **OpenVPN** can be used to create secure end to end connection in **remote access** (en.wikipedia.org). It provides encryption facility using **OpenSSL**. Now it is more secured comparing to other VPN technologies.

All these security requirements are shown in this network diagram. So, it can be said that the design of iSee clinic network fulfill all the mentioned security requirements.

Task 4

By above explanation, it is seen that iSee clinic network is analyzed properly and vulnerabilities of the network are identified. Also, the solutions to prevent the threats are recommended. Now how these security solutions will be maintained in the future are explained here.

- Regular **vulnerability assessment** and **security audit** should be done to identify the weakness of the system.
- Standard **security policy** like back up policy, restriction policy including limitation of using removable disk and downloading should be established.
- **VPN and EFS** technology should be deployed strictly.
- Strong two step **authentication** should be established.
- Regular **monitoring** of server and hardware should be done to identify threats and prevent theft.
- **Training** should be provided to users about the secure use of network.

Task5

a) The problem that I faced badly to complete the assignment is the limitation of time. It made hard for me to analyze the whole scenario properly in this time and also visualize some diagrams to explain the security terms more perfectly.

b) If I were to start the assignment at very beginning, I would spend more time to analyze the scenario firstly. Then I would have been analyzing the threats and measuring their consequences for particular days. So all the security measures would be explained well. Finally, I would try to visualize the main security terms for explaining them perfectly.

Conclusion:

At the end of the discussion, it can be said that the network of iSee clinic will be safe and secured by maintaining above recommended security solutions strictly.

Bibliography

Retrieved from datarecoverylabs.com:

https://www.datarecoverylabs.com/hard-drive-failure.html

Retrieved from security.berkeley.edu:

https://security.berkeley.edu/resources/best-practices-how-articles/securing-remote-desktop-rdp-system-administrators

Retrieved from techgenix.com:
http://techgenix.com/securing_remote_access_connections/

Retrieved from advisera.com:
https://advisera.com/27001academy/blog/2011/10/25/what-is-cybersecurity-and-how-can-iso-27001-help/

Retrieved from gov.uk:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395717/10_steps_infographic.pdf

Retrieved from en.wikipedia.org:

https://en.wikipedia.org/wiki/OpenVPN