Coursework 1

**Part 1**

A description of the network is each office will have x number of pcs all connected to a switch and that switch is connected to a router and that router can communicate with the other routers on the network through the use of a main router meaning all the offices are connected and can interact smoothly.

The hardware and topology requirements to set up this network is the star topology as in the office there will be several pcs connecting to one switch and that switch connecting to a router and the router sharing information between other routers.

This here is the network I designed in cisco packet tracer to run and connect all the offices together:

A picture containing text, sky, map, light

Description automatically generated

**The various network protocols used on networks are:**

* DHCP - assigns IP addresses to endpoints so they can communicate with other endpoints over the internet.
* TCP/IP – 4 parts used to transport packets over a network.
* HTTPS - standard protocol to secure data being transferred over the internet.
* RIP – determines the optimal path for data to take while being transferred over a network.
* FTP – protocol used when transferring files over the internet.
* POP3 – protocol used for receiving an email.

Having adequate network security is import as if your network isn’t secure then the data being transported on the network can be easily accessed and can be used to cause harm to people. When setting up a network you need to know the vulnerabilities of the network so you can plan around them to try limit potential attackers as you don’t want sensitive data to be able to be intercepted.

Hardware security is protecting your physical devices (hardware) from unauthorised access. Hardware security within a network could be something like a proxy server or a firewall, it could also be sealing usb ports on pcs so employees couldn’t potentially insert malware directly into the pc and bypass the network security. Another layer of hardware security is having strong passwords that aren’t easily crack able so hackers can’t easily gain access into the system.

One factor that can challenge my network is its security as the network has to be made secure to keep people gaining unauthorised access and if security isn’t factored in while making the network it will have to be added in later and may interfere with user experience.

Another factor is scalability of the network as the network is over 4 offices it has to be able to grow and not break furthermore a scalable network will be more cost efficient.

Finally, a factor that challenges the network is its ability to evolve and improve as cyber is a fluid situation and people are always changing their methods of attack so the network has to be able to adapt to what is being used at the time

Part 2

Dear CEO,

The stance the company should take with regards to customer data is there should be sufficient protected to that all the cyber laws; those laws being the 1990 computer misuse act and the GDPR 2016 act which builds upon the CMA act. The other law to abide by is the 2018 data protection act, as the company deals with consumers financial details, you can do this by limiting employee access to the financial details and having them secured on an encrypted data base and keep a log of who accessed the database and when and where they did it from. It is vital these laws aren’t broken as the company can be held financially liable for any damages caused by a data breach and outside of law the public image of a company losing its customers financial records would ruin the company image and lead to a drop in customers.

As CEO you should also want to have internal policies within the company to boost cyber security and force staff to undergo training to minimise the chances of them falling victim to an attack. One policy could be no external drives (USBs) are allowed to be inserted into PCs as this is an easy way to bypass the networks defences and insert malware directly into hardware, another policy could be you have to connect via a VPN to encrypt data being sent so even if its intercepted they won’t be able to read it, a third policy could be to implement regular staff training to keep them up to date on the current cyber threats and to make sure they don’t get comfortable and slip up and give them a way to learn in a harmless environment without serios consequences as without regular training staff may be more vulnerable to phishing scams which are the easiest and most common entry into systems as it relies on human error which will always be present regardless of a networks security, another policy you could implement is no connecting to the network without using company issued devices that way you can track activities on those devices to minimise misconduct and check if staff are following the 10 computer commandments and properly dealing with customer information they should also not be allowed to use these devices outside of the office as bringing them home may cause issues if they are lost or stolen.

The company should also be ethical about the information they collect and how they collect it and use it as customers trust the company and it would be unethical to break that trust or not show it the respect it deserves; all staff members should be educated on the 10 commandments of computer ethics so they are aware of how to ethically use a computer. Furthermore, staff should tested for their moral values/codes and see if they align with the companies moral values/code as staff should be held to the highest professional standard as without proper moral values / ethics the consequences are incompetence which can lead to scandals and then law suits due to breaches of the law.

There should be access control restrictions should be added as it adds levels of security as you need to have the right security clearance to access company files. This will help to prevent low level stats employees from being able to access the same information as the top level employees as they don’t need to be able to access it, if they were able it would decrease overall integrity of the system as it become more vulnerable to attacks due to more information being available. Furthermore, a low level employee shouldn’t be able to access peoples bank details as they could either expose them knowingly or unknowingly both of which shouldn’t happen and is illegal. There should also be network access control added to the network as it provides layered security further protecting any data on the network as potential hackers have to break down more walls than just the one and having access to everything which can help to minimise and contain damages if an attack is successful on the network.

Finally monitoring employees activities should be happening as you can see what files an employee accesses to source data leaks and help monitor activity to see any suspicious movements on the network, moreover you should also log which files are accessed by which computers on the network and at what times this helps to build a better picture of the networks usage so if a cyber attack happens it can be easier to trace due to you having all the information in real time.