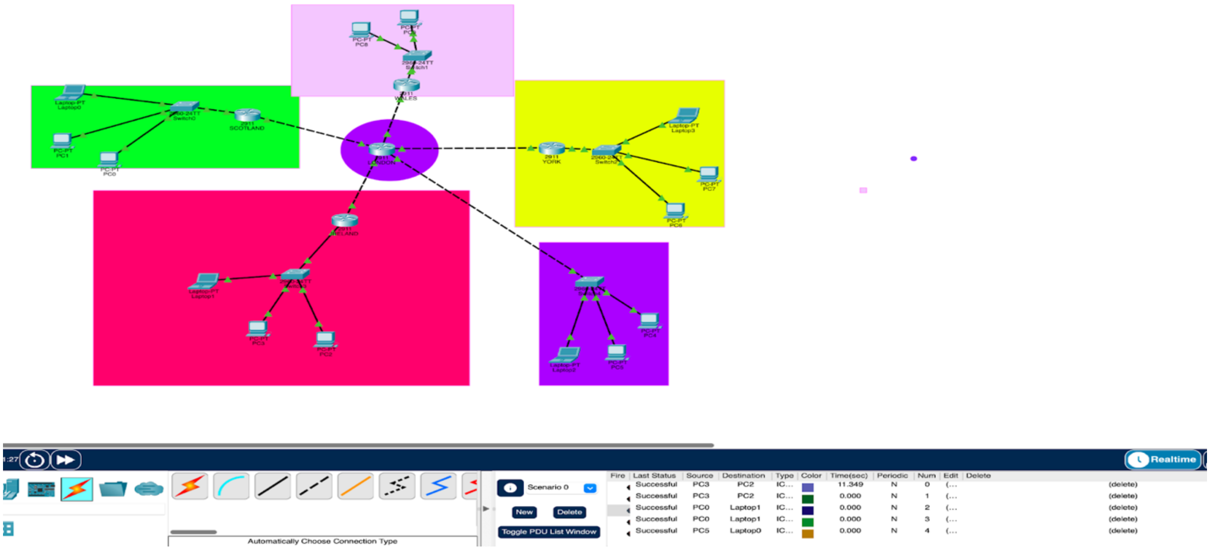
Title: Cyber security plan – Coursework 1
Student name: Sawsan MOUNES
Student ID: MOU23620003

PART 1

The cybersecurity consulting company's network plan aims to establish seamless communication between the branch offices in Scotland, Ireland, Wales, and York and the main office in London. This centralization, with London as the central hub, ensures that all clients, including branch offices, can access and use shared data resources. The network plan incorporates a Wide Area Network (WAN) to facilitate communication between all locations, while each office uses a Local Area Network (LAN) for internal communication purposes. In addition to connectivity, the network plan includes functionalities such as software and hardware sharing, allowing users to access applications from the main server. Security measures are crucial in preventing unauthorised access and potential hackers, especially considering the company's focus on cybersecurity. Moreover, backup solutions are implemented to mitigate the risk of data loss in the event of system failures. Data-sharing capabilities enable efficient collaboration between offices by facilitating the sharing of files, presentations, and projects. Considering the performance aspect, high-performance computers are used to support cybersecurity consultants in defending against threats effectively. Scalability is also to be considered, particularly when accommodating growth such as hiring new employees or adding more PCs to expand the network's size.

We intend to implement a star topology in our network plan, where each office will be connected to a central hub. This setup offers several advantages, one of them is that if a node fails in one department, the other nodes will remain operational, improving reliability and independence. Additionally, it is a cost-effective solution. Moreover, the London office will have the capability to administer and monitor the network, improving security measures to prevent unauthorised access and safeguarding the company's confidential information. Hardware devices to create our star topology network will include a central hub, Network cables, Switches, NICS, Router, VPNS Firewalls, PCs and laptops

Cisco packet traces design:



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
◂	Successful	PC3	PC2	IC...	🟪	11.349	N	0	(...	(delete)
◂	Successful	PC3	PC2	IC...	🟩	0.000	N	1	(...	(delete)
◂	Successful	PC0	Laptop1	IC...	🟦	0.000	N	2	(...	(delete)
◂	Successful	PC0	Laptop1	IC...	🟩	0.000	N	3	(...	(delete)
◂	Successful	PC5	Laptop0	IC...	🟧	0.000	N	4	(...	(delete)

TCP/IP, a common protocol in modern networks, enables seamless communication between devices across the network, while Internet Protocol (IP) facilitates the transmission of data packets between computers. This setup is particularly advantageous for branch offices as it efficiently manages large volumes of devices and network traffic, ensuring error-free data transmission. However, another protocol that works similarly to TCP is UDP (User Datagram Protocol). It sends packets from one device to another device. While more expensive, UDP is cost-effective as it has higher speed than TCP and supports video and audio, which can support the company with conference calls, also enabling other offices to communicate with each other but I would add both as TCP is more reliable than UDP. Furthermore, the Domain Name System (DNS) plays a crucial role by translating domain names like https://www.roehampton.ac.uk/into corresponding IP addresses, allowing easy access to online resources. This functionality supports the cybersecurity company by facilitating quick and secure access to vital online resources for its employees.

Security software such as antivirus applications like McAfee and Norton should be incorporated into the cybersecurity infrastructure of the company to prevent spam, viruses, malware, and potential phishing attacks. Furthermore, by implementing firewalls, the company can prevent unauthorised network traffic, reducing the risk of cyber-attacks and malicious software in the computer network. This also helps in safeguarding sensitive data from being leaked outside of the company. It's not just about implementing security measures on laptops but also educating employees about their role in maintaining security. They must raise awareness among employees regarding their responsibility to keep company information secure. This involves adhering to policies, signing agreements, and following company procedures. To reinforce this, regular training sessions should be provided every six months to ensure employees remain up to date. Additionally, Employees working at the company should follow basic security measures such as using robust passwords and ensuring they change their passwords every six months to prevent unauthorised access. Implementing two-factor authentication will help mitigate security risks, making it more challenging for unauthorised individuals to access their accounts and sensitive data.

Hardware security is essential for preventing unauthorised access and protecting against. cyberattacks in networks, particularly for cybersecurity firms. One key strategy is to disable automatic connections, which prevents employees from unintentionally connecting to unsecured public Wi-Fi networks outside the office, reducing the risk of potential attacks. Additionally, encrypting data stored on hardware devices is crucial as it prevents potential hackers from accessing sensitive information if a device is stolen or compromised. Another an important consideration is mitigating backdoor risks, which hackers exploit to gain unauthorised access without the user's consent. This can be addressed through the implementation of robust security measures such as firewalls, continuous monitoring, and strong passwords. Consistently maintaining these practices throughout the cybersecurity company's network ensure reliability and adherence to the principles of confidentiality, integrity, and availability (CIA)Integrating these security measures into our network plan across all. branches and the London office ensure smooth operations and build trust with clients.

Even though my proposal outlines security issues however my proposal can be challenged by our infrastructure especially since it is 4 branches, we are still vulnerable as data breaches can still arise to mitigate this we should log monitor to check for any anomalies within the system such as unknown trafficking or any potential reg flags that could across as cyber threats.

Expanding the network size could potentially challenge our proposal by slowing down network traffic, leading to congestion and slower communication. Additionally, as more devices are added, the network becomes more susceptible to cyber-attacks. To mitigate these challenges, we plan to expand our hardware infrastructure, including routers and switches. Furthermore, integrating cloud computing into our network design allows for dynamic scalability, accommodating the increasing storage and data needs. Cloud services provide accessible storage and data resources for employees, enabling them to access information from anywhere.

Another issue that may occur is the reliability of the network plan, specifically the star topology used. If the central hub fails, all four branches will fail, resulting in a loss of communication. To counter this potential problem, further steps can be applied. One alternative is to incorporate additional power supplies and construct a backup central hub at the London location. Furthermore, implementing monitoring systems for the central hubs would be a proactive method for detecting and addressing potential future difficulties.

Title: Cyber security plan – Coursework 1
Student name: Sawsan MOUNES
Student ID: MOU23620003

PART 2

Beyoncé Giselle Knowles-Carter
ireland Rd
Busch Corner
Ireland
TW7 5NA

Returning address:
Mounes cyber security consultant
Roehampton Ln
London
SW15 5PH

Date:20/04/2023

Dear MS.Knowles-Carter, (CEO),

We appreciate you entrusting Mounes Cyber Security Consultants, during our visit on April 15, 2023, with the worries of your firm. After conducting a comprehensive evaluation of your organisation's network and processes, it has become apparent that substantial enhancements are required to increase data security and ethical handling. Our main goals are to protect client information, make sure that legal protocols are followed when managing private data, and establish confidence between your business and its clients to maintain your reputation.

A large size of the network used by the company is open access. This strategy does, however, come with some risks. Since open networks don't have encryption, data interception and unauthorised access are possible. As a result, private data like bank account information and addresses could be compromised. Furthermore, spam and malware can infiltrate open networks, endangering the security of the business and compromising the integrity of customer data. It was also observed that many workers have unrestricted access to other company computers. Such unrestricted access increases the risk of unauthorised data access and manipulation, potentially endangering the confidentiality of client information. Due to the ambiguity, this seriously jeopardises the system's overall security regarding the motives of staff members. Moving to a private network, where there is more control over traffic and packets sent to company devices can be monitored, is what I would suggest mitigating these. Further enhancing data security and reducing the risk of unauthorised access and customer data protection can be achieved by implementing extra security measures and access controls, such as mandating passwords and two-step verification for all employees.

Your business must handle data responsibly to prevent legal fallout from data integrity and data privacy violations Sadly, a lot of customer records have errors in them that are frequently missed by staff members, maybe as a result of human error during data transfers. Employees should be trained to thoroughly check for errors and validate data frequently to reduce these risks. Promoting frequent data backups might also help to avoid loss or corruption. These steps not only reduce errors but also show the business's dedication to treating data ethically, preserving its reputation, and guaranteeing customer privacy. This will enable you to build trust and integrity between you and your customers. Building trust and integrity with clients is critical, particularly given the quantity of information they provide to the organisation, such as their contact information. However, it appears that this trust has been breached, potentially infringing on their privacy rights under the General Data Protection Regulation. This legislation requires data to be managed securely, protecting against unauthorised processing, access, loss, destruction, or damage, especially fraud. To avoid legal complications, the company must strictly follow these regulations. To reduce these threats, set access limits, encrypt critical data, and strengthen physical and network security. These actions can help prevent unauthorised access and data breaches, therefore securing customer information and ensuring compliance with data protection standards.

Finally, improving security measures in the finance industry by monitoring log files allows for the detection of unknown, harmful attacks and cyber threats. This monitoring enables our organisation to identify any vulnerabilities in our security infrastructure. Furthermore, by supplementing the logs with records of data access, we can trace who has accessed critical information, lowering the risk of data compromise within the organisation. Furthermore, imposing restricted data access and limiting it to staff with relevant responsibilities will reduce overall data access while strengthening our security posture.

In conclusion, by correcting the concerns we observed to prevent future issues in your firm, we hope that you would consider our recommendation to protect your data and consumer data by safeguarding it and adhering to cyber laws.

Sincerely,
Sawsan Mounes,
Cyber Security Consultant.
Contact Information: 07539176868