Michael Labate

11/12/22

Technology report James Otis tax associates

Based on the requirements provided, I will describe the hardware and software necessary to allow the employees at James Otis Tax Associates to effectively complete their tasks. This report will be segmented into paragraphs. The paragraphs will be as follows, requirements, hardware, software, network, security and VPN basics. The individual components will be in **bold,** to easily identify them within the report. There is also a diagram created via Microsoft Visio to visualize the recommended network configuration. It has a color-coded key at the top right. While discussing network requirements, various components in the paragraph will be color coded. For example, Router or Firewall, will be color coordinated to match the diagram. First, I will go over requirements as prescribed by the client.

As stated in the requirements, three employees must have a workstation connected, with the ability to share information and files securely. CPA, Tax specialist and Data-Entry Specialist are described in the requirements. A way to securely store large amounts of data is not mentioned, however I assume that will be vital to the operation of this company. Also, we have been tasked to describe each recommended component and provide specific software programs for utilization within the company. Finally, the client stated the company is growing rapidly and just opened a new office. Based on this statement, I have decided to design a network allowing communication amongst current and future offices. I will now describe the hardware components required to meet these specifications.

First, three **desktops** will be required. Due to the sensitivity of information, wireless is not recommended. Each workstation will also require an **IP Phone** for communication with customers. An IP Phone uses internet instead of phone lines to operate. Additionally, each workstation will require a **keyboard, mouse** and two **monitors.** Two monitors per workstation will allow employees to more effectively multitask. **One Fax/Copier/Printer combo** will also be a requirement. This would be essential for professionally sending documents to customers, making copies and printing tax documents. The remaining hardware will be described in the network section of this report.

The first software required would be the most updated version of **Windows operating system** (OS). Along with the OS, **Microsoft Office 365 Business Premium** is essential. This version of Microsoft Office includes Outlook, Word, Excel, PowerPoint, OneDrive, Teams, Bookings, Forms, Lists, Planner, Exchange, SharePoint, Publisher, Access, Intune and Azure Information Protection. SharePoint is a tool that will allow all employees to access shared files over LAN or WAN. This will allow the company to expand without having to add servers to store information for each office. **SharePoint** also allows the configuration of files to be accessed by certain users. This will allow the company to departmentalize information based on job roles and permissions. **Microsoft Teams** could also be a useful tool for an expanding company. This will allow upper management to host meetings with other branches without having to travel. Another powerful tool is **Microsoft Bookings**. Customers can make or change appointments by accessing the company’s Booking account. This will streamline the process for customers and employees. This also integrates with Microsoft Teams allowing virtual meetings with customers. This gives customers a useful and convenient interface and could potentially attract more business because of the human computer interaction aspect (HCI). The final software recommendation is called **CCH Axcess™.** This program is specifically designed to be used with cloud-based services. It offers electronic filling and will find common errors and alert the user. This will improve productivity and reliability on tax return forms.

For network requirements, not much hardware is needed because of the cloud-based and mesh-based system. There are a few components that are required. One is a simple eight port router. This will allow enough ports to connect all devices into the network. The router will direct traffic from the LAN to the WAN and vice versa. A modem will connect to the internet service provider (ISP) and to the cloud-based servers. The rest of the networking components will be covered in security.

Network security is arguably the most important aspect of a business. Because of this, I incorporated a multilayered and redundant security system/network. The first layer of security will be a high-quality **antivirus software** (AV) on all devices. An AV will also include a software firewall which can prevent unauthorized users from infiltrating the LAN. Adding an external firewall will also be beneficial to the security of the LAN. If the external firewall is breached, the internal firewall installed on each device could potentially eliminate the threat. External firewalls also allow manual configuration which will allow system administrators to control and monitor internet traffic. Another security recommendation would be a system called **Perimeter 81**. Perimeter 81 has multiple tools that can be utilized to improve security, redundancy, and control of the network and infrastructure. I will describe only a few. One is dedicated servers with dedicated IPs. Basically, the only users using the server are people connecting through the dedicated VPN. This also adds flexibility for employees working from home. It will allow employees to securely work from their personal computers. Also, the two-factor authentication is a superb feature. When employees log in their Perimeter 81 account, they will receive a text message or push notification on their smartphone displaying a security code. This security code will be required to access sensitive company data on the VPN. Another feature is Split tunneling. Essentially, this would allow you to choose what subnets you want to use the VPN tunnel on. For example, if you wanted sensitive traffic to be encrypted and sent through a VPN, while standard traffic is routed normally, this allows you to do it. This can optimize network performance. However, split tunneling can be a security risk if not properly configured. Site to Site is also offered from Perimeter 81. Site to site allows networks to communicate directly to each other. This keeps your sensitive information off the public internet. Another feature that could be used is user management groups. This allows certain users to only have certain permissions. This would be vital for a company with multiple roles requiring different permissions. Overall, Perimeter 81 allows scalability, security, and control of your network. I will include a diagram of what data flow would look like if the company expanded.

Lastly, I will explain the basics of VPN’s, Split tunneling, Data encryption, Site to Site and the diagram labeled 5-1 data flow attached. A VPN is a virtual private network. This routes traffic through a virtual tunnel to a VPN server before retrieving information from the public internet. This masks your IP address and your data. Not all VPNs encrypt data, but Perimeter 81 does. The client requests that all data be encrypted to the server. After that the server and client agree on an encryption key, and encrypted data is sent over the network. The only two entities that should have this key are the two communicated. Encrypted data is essentially jumbled data that is not able to be deciphered easily if intercepted. The key tells the systems how to decrypt the data. Finally, site to site communication creates a virtual network between two points. This can replace MLPS if desired. Diagram 5-1 data flow represents how data would flow using a VPN with split tunneling, Site to site, tunneling and encryption. The blue lines represent traffic flow with split tunneling using public internet. This data is not encrypted or tunneled. The red lines represent data being tunneled, encrypted and sent through a VPN. The yellow represents data being sent tunneled, encrypted, and set directly to the end point using split tunneling.