Building on prior success

Technology, Information Technology

The network operating system that could be suggested for incorporation into the company systems would be Microsoft's Windows Vista. This network operating system presents users with numerous capabilities, essential for performing various daily company functions. The Vista version of operating system contains numerous security protocols that could significantly enhance security of the network system once installed. Protecting the contained data from unauthorized access remains critical to the success of the network; therefore, installation of an operating system with security protocols remains essential (Hallberg, 2009). This version comes with a secure socket tunneling protocol from Microsoft, which would work efficiently with other supporting security protocols in providing secure connections. This tunnel provides a mechanism for safely transporting encryptions through almost all proxy servers and firewall.

Incorporation of new servers into the system would include numerous activities of upgrading the current system, and ensuring compatibility with the operating system. Extra servers remain fundamental in increasing the available storage space within the company network system. Installation of extra servers would follow centralization of the servers; hence ensuring information retrieval from a central location. The company's head-office could potentially serve as the central location for new servers. This would essentially enable regional offices' users to access information from company, servers through the internet. Similarly, remote employees would also access required files contained in central servers from different locations. Central server installation remains fundamental in enhancing information security as information could be protected from a single source

(Hallberg, 2009). Confidentiality of the information could become immensely enhanced through sender authentication at the central server, enabling secure information movement.

The best way for employees to remotely access Ocper Inc. network would be through utilizing mobile virtual private network. Mobile VPN setting functions efficiently in situations where the endpoint VPN contains multiple access points. The mobile network can also be accessed using cellular devices carrying data between several Wi-Fi access points. These individuals could utilize modern I-phones, with capability to access VPN connections, as the network connection enables seamless roaming between networks through utilizing wireless connections. The advantage of utilizing this connection remains the ability for the network to connect between different IP addresses without losing information contained in other applications. The mobile VPN allows users to maintain several applications continuously open. While performing this function, the network also allows passing of data, securely over public networks. This capability would immensely assist employees Ocper Inc to access the network continually from several remote locations. Within office settings, however, the Virtual Private Network could be accessed through the conventional connection. This connection presents numerous limitations, making connections insecure when establishing remote connections. When the network becomes interrupted, information could be lost or computing devices could crash (Hallberg, 2009). This network connection, therefore, becomes limited to desktop computers and immobile computing devices. The mobile Virtual Private Network proposed, could be utilized on different mobile computing devices, including laptops, and mobile phones among other devices. These devices could be efficiently utilized by employees in remote areas for accessing the company network. Majority of these devices have the capability to access documents and files created using the Windows Vista operating system; hence employees would not encounter compatibility problems.

References

Hallberg, B. (2009). Networking, A Beginners Guide, Fifth Edition. New York: McGraw-Hill.