With use wep to encrypt data, and should

With the given prompt, it had to be determined how best to handle network security for an online streaming media company. As a company that relies heavily on third party vendors, it’s important to focus on the security risks of transferring data outside the company’s firewalls. This includes the security risks of using email and FTP; similarly, the security precautions for networks inside the workplace environment should also be considered. Email is one of the most commonly used methods in a business environment for data transfer.

Unfortunately, email poses a lot of threats to a company’s safety. Messages containing critical company information can not only be sent to an unknown external party but can also hold a multitude of viruses. It can be quite simple to gain confidential data of an employee from email, such as their username and password. A solution could be finding a way to identify the source of the sender. A good example of this is using an encryption program such as Pretty Good Privacy, or PGP. In addition to an encryption program, sending out the company’s security guidelines to the employees should also be considered. FTP is similar in that it is a risk to company data.

FTP is not encrypted, and therefore it is not an ideal choice. MFT is a much better option, as it encrypts files and alerts the sender if a problem arises in the file transfer. Understanding the risks of certain network environments inside the workplace can be beneficial to the company’s health as well. VPN networks are considered to be the equivalent as bringing your own laptop to work. It helps in regards to keeping secure from an untrusted network, but not from an untrusted device. There is nothing that can stop malware located on the untrusted device from extracting access credentials or

copying critical work files. Using company regulated devices can assure that the company’s data can remain secure.

In general, networks are susceptible to many issues. One of the issues arises from the firewall itself. In many instances the firewall is not properly set up, which results in creating an entrance for many security risks. Another risk to consider is using little, or no wireless encryption. Many companies still use WEP to encrypt data, and should consider the benefits of using WPA. The company needs to primarily focus it’s efforts on managing the threats the third party vendors pose. Knowing the vendor’s and the company’s security risks could prevent the scenario in which the prompt addresses.