[Title Here, up to 12 Words, on One to Two Lines]

Author

Institution

Creating and Communication a Security Strategy

The efficiency of system administration hinges upon the network security. There are numerous cyber threats being faced by business networks in contemporary time. However, to avert such threats network security is pivotal for designing security strategy. No matter how big or small the business is, it has to be ensured that the network is secure enough to avert spoofing and data stealing. One of the latest incidences of data breaches is ‘WannaCry Ransomware’. Data was locked on thousands of servers across the world due to ‘WannaCry Ransomware’. The development of sophisticated hacking skills by hackers necessitates all business to strive for effective network security. Most of the security breaches are testament to such sophisticated skills.

This essay intends to discuss the security strategy of Dropbox business. Dropbox Business is a package offered by Dropbox for file sharing, and most companies and enterprises use Dropbox. Any company or enterprise, as a client, can use Dropbox to sync and share files easily. Besides, Dropbox also provides its clients with abundant space for data storage, and collaboration between the employees of the company or enterprise. The essay will be focused upon the protection and security of cloud computing that Dropbox uses for file sharing and storage. The potential threats to the cloud system and how could such threats be averted will be discussed as well.

# Potential Threats to Cloud Computing

Ransomware is a threat to any company’s cloud storage as that is just an extension of its network. Ransomware seeks out connections and exploits them. If the company maps a drive to its cloud storage then it will become infected along with the rest of its computer and/or network. If the company uses a Sync tool to synchronize its local files to cloud storage (One Drive, Dropbox, and others do this) then that too will become infected. Another potential threat to the cloud is crossover traffic bleed. Crossover traffics bleed happens when a company has a memory overflow in a shared cloud computational space. Owing to crossover traffic bleed data could be obfuscated.

# Security Strategy

Equipment glitches and installation of piracy software invite most of the breaches in network security, however, inadvertently. Some default security holes of TCP/IP protocols and operating systems can also lead to a network security breach. And then, we have the advanced evasion techniques (AET), which combines different evasion methods to devise a new technique to bypass an information security system. Hackers can breach business network security in number of ways such as; password attacks, spoofing of IP address, social engineering, and Denial of Service attacks. However, the steps for effective security strategy are as follows:

* Secure data sharing: A sound network security infrastructure in place could ensure secure data sharing.
* Managing data traffic: Systems exposed to a high level of traffic are more prone to network security attacks. So, for an improved user experiencing without putting a website or system on risk, reliable network security is important.

Data breach would not surprise any company as it is not something very unique, and most of the companies have witnessed security breaches in their networks. However, the way by which hackers encroach on business security is worth mentioning. More often than not companies would themselves caught in the undertow following the data breach, because undoing its aftereffects is very difficult. Undoubtedly, prevention is the best cure! If any company’s employee loses his/her unencrypted laptop, or the employee witnesses a hacking attack on the device, then network and data breach would be easy. Besides, if there is not CASB solution in place then tracing data breach would be much more difficult and time consuming. In addition, company may find itself in zero-solution zone sans any adroit security solution. By integrating multiple layers of defense in the network, and by implementing controls by each network security layer such network security breaches can be averted.