**MEMORANDUM – 2 MINUTE BRIEFING 4**

**TO:** CASEY G. CEGIELSKI, PH. D, CISSP, CISA, CRISC

**FROM:** CENSORED

**DATE:** 10/2/19

While Asymmetric Key Cryptography is a very secure form of encryption, it is also inherently slow (about 1000 or more times slower than Symmetric Key Cryptography). If you already have top-of-the-line systems then this might not be a bad idea (since it will be a bit faster with more computing power), although in my opinion it is not wise to make all this data depend on asymmetric keys. While symmetric keys are a faster option, they only encrypt the data and restrict its access; they cannot provide proof of origin for the data, meaning we cannot prove the integrity of the data we’re protecting with it.

Symmetric keys are very fast at encrypting data, are very difficult to break, and tons of tools used for Symmetric Key Cryptography are freely available online. There are some downsides that come with its use: the keys can be used to encrypt and decrypt, the number of keys grows exponentially with each user added (the main problem here), and the limited security aspect that was mentioned earlier. The main problem makes it difficult to use symmetric keys in this situation; while it might encrypt the data faster, there will be an inherently large number of unique keys in use (with only 1000 users we would have 499,500 keys). The problem with this is that the keys and data must be delivered separately; that means you will be receiving millions of keys at your centralized transaction processing center.

Is this negligible in comparison with the problems faced by using Asymmetric Key Cryptography? Yes! Time sensitivity is the main factor here, and Asymmetric Key Cryptography would be much too slow for all this data. While asymmetric is preferable for security, in this situation it would not work at all due to the amount of time it would take to encrypt/decrypt the data. It is also important to note that Asymmetric Key Cryptography is a one-way communication, which is exactly what we want; all the stores are only sending data to corporate but never receiving any, so why would we use Symmetric Key Cryptography (2-way communication)?