**MEMORANDUM – 2 MINUTE BRIEFING 1**

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

**FROM:** CENSORED

**DATE:** 8/26/19

A risk assessment is necessary because the impact a vulnerability/attack can do to a business is monumental. A risk is the likelihood that a loss will occur, and losses occur when a threat exposes a vulnerability. A threat is any activity that represents a possible danger and a vulnerability is a weakness in the system. A risk assessment will help identify potential risks and work on accepting them, mitigating them, transferring them, or avoiding them. We can do this by identifying which risks are manageable and therefore acceptable to ignore, which ones are severe enough that they must be transferred for something else to manage, and which ones must be avoided/mitigated entirely. If a risk is not properly calculated and a vulnerability is exploited, then loss will occur and there will be a compromise to business functions or assets as a result.

Some other safety nets we can implement to aid in risk management are safeguards/countermeasures. A safeguard/countermeasure is the safety net itself – it is what guards the business when the above protective layer is broken through. An example of this could be encrypted passwords – even if a vulnerability is exploited and employee/customer data is stolen, the passwords are encrypted and are much harder to use for large attacks. This provides an extra layer of protection, so that the attacker does not have all employee/customer passwords immediately and must individually and manually decrypt each password.