**MEMORANDUM – 2 MINUTE BRIEFING 2**

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

**FROM:** CENSORED

**DATE:** 9/4/19

The most important and common vulnerability/threat pair is when a disgruntled ex-employee (the threat) still has an employee login to the system (the vulnerability). It is easy to mitigate; just change the login information (or delete the account entirely, which would be the preferred option) after the employee is terminated. If this is not done then there will be a huge chance for a threat action to occur, namely the ex-employee accessing sensitive customer/employee data and utilizing it for his own selfish gains. This could lead to a personal attack on a customer or employee, or even a large attack on all persons affected if the employee were to sell the data.

Another important but less common vulnerability/threat pair is when a hacker (the threat) gains unauthorized access to a company system through a flaw in the system design (the vulnerability). The vulnerability could be anything in this case, such as non-updated software, hardware vulnerabilities or even a 0day (a new vulnerability that has not been mitigated yet). If the hacker knows about this vulnerability or stumbles upon it (say, while using the e-commerce website), they can exploit it and steal or destroy sensitive data. This is harder to protect against, since there is a very wide range of possible vulnerabilities the hacker could exploit, but if the e-commerce website and application are secured from these attacks enough, it should not be a common occurrence. The public-facing servers are the most at risk for this vulnerability/threat pair, as public-facing servers are open to attacks executed by code if they are not secured properly.

The last (and sadly the most common) vulnerability/threat pair is negligent people (the threat) accidentally or purposefully exploiting a vulnerability. This is usually in the form of a workplace accident, like if an employee were to trip and fall over a cable from one of the systems. Even if the event was an accident, damage was still done to an employee and a system as a result of it. There are strict regulations that must be followed so these physical accidents do not happen as often, such as cords being tucked away out of the walkway, no liquids being kept near systems, and only placing systems on sturdy surfaces. While accidents cannot be mitigated completely, they can still be prepared for and hopefully mostly prevented; the same cannot be said for purposeful events of this nature. There must always be emergency situations prepared to handle these events, as it is highly likely that a fire could erupt, or a customer/employee may be badly injured. While these latter situations are less common and cannot be mitigated at all, they can at least be handled safely and be prepared for.