Name: CENSORED

Date: 8/28/19

Class: ISMN-5730

**THINK PAIR SHARE 1**

The three types of possible threats that should be watched out for are unauthorized access, unauthorized alteration, destruction, or disclosure of information, and insertion of malicious programming code. The first threat is experienced when either an employee or an outside actor attempts to gain access to employee/customer records. The second threats can take place after an attacker has gained access and has then decided to leak/change/destroy any information they discovered. The final threat is the most harmful, as it can destroy a machine while still getting the attacker what they’re after or even take full control of a machine.

The impact of the first threat is minimal; the attacker may have access but does not necessarily have the means to modify/delete any existing records. The impact may still be worse if they describe what information they discovered, which could lead to a breach in security. The second threat impact is medium at best, as keeping backups of the information stored on the servers can mitigate damage done from modification of this data; however, the damage done by this information being stolen and used (like bank account information) can be very high. The final threat has the highest impact, and if it is executed on one of the local machines (like an ATM or any bank computer) then it can be incredibly hard to fix. The first and second threats are probably the only threats that are likely to occur; the third threat can happen, but with good physical security it becomes nearly impossible for anyone to execute without a decent amount of unsupervised experimentation with the machine. The final threat becomes more likely since there is a mobile banking application, but since this is developed and maintained by a third party it can be assumed that this will not be a possible attack vector.

I personally would rank the second threat as being the most important to prepare for due to how often it may happen, with the final threat being the least important and the first threat being the second most important. I would give these rankings because any form of unauthorized access is a common problem in any business that uses computers, but injecting code is incredibly rare due to someone having to write code specifically for a certain machine. Other types of unauthorized access happen all the time due to negligent (or in some cases malicious) employees, but injecting code would have to be very professionally done and is therefore not something that needs to be constantly monitored for.