Name: CENSORED

Date: 9/25/19

Class: ISMN-5730

**THINK PAIR SHARE 3**

The access controls already in use by your company are access initiation (i.e., a user registration procedure), a unique ID system, account monitoring, automatic password expiration (and the use of a password-based login), card key systems and sign-in sheets. The way we categorize each is by their control category and by their type of control. For example, a user registration policy could be recognized as an administrative preventative form of access control, the ID system could be seen as a technical detective type of access control, account monitoring could be an administrative detective form of access control, the use of passwords in general (alongside password expiration) could be consider a technical preventative type of access control, the card key systems could be seen as physical preventative and a sign-in sheet for visitors could be considered physical detective.

There are a variety of threats that can target these forms of access control. For example, one threat that may be harmful to a password-based login are password crackers; they can perform dictionary attacks or similar attack vectors to crack easy to guess passwords used by employees. The only way to circumvent this threat is to enforce employees to use strong passwords that have not been used anywhere else. Another threat to password-based login is the art of shoulder surfing, although this can be mostly vanquished by the usage of special screens that only allow the user to view what is happening on the system. Another huge threat that may have slim chances of happening (but would be devastating if it did happen) would be the usage of malicious software; it could be installed by an employee or a completely external threat actor, but the damages to the company would be major. This problem can be circumvented by installing strong anti-virus software on every system as a precaution.

The biggest attack vector that your company is open to is social engineering. Social engineering is the art of manipulating people with speech and actions to ultimately achieve some goal not known to the other party. Attackers can use this to pose as a high-ranking employee with the company in order to scam valuable company information out of another employee, although I feel the use of ID cards will help mostly circumvent this. This is still a huge attack vector if it was to be exploited physically; CCTV cameras would mitigate this. Without cameras, someone could steal an ID or lie on the sign-in sheet and there would be no proof that they did it. One further attack vector that could be exploited is poorly updated software/operating systems; if the systems are out of date, they could be open to older vulnerabilities that could be devastating (for example, an old privilege escalation vulnerability; if this is used on the system after gaining access to the generic manufacturing login, admin privileges could be gained). The last (and possibly the least threatening) threat to access controls is the art of dumpster diving, where important documents or company information can be found. This can easily be mitigated by shredding all important documents and being mindful of what ends up in the trash.