Severe

Leaving a network unprotected from external threat.

I picked this as the biggest threat to a corporate headquarters because of the value of the information being stored on the network. There is no greater asset to a corporate headquarters than the information that is being sent and stored on their network.

Phishing scam on company computer

I put this in the emergency category for similar reasons as the first one. Even if the network is very secure and there is no direct way to hack into in without being on the network, a phishing scam can bypass this problem by gaining direct access to the user’s computer and attacking from the inside out.

Middle

shared access to deliveries

I put this in the frequent and moderate section because it is something that happens in almost all offices but is not really an issue unless there is an actual organized effort between the delivery person and someone wishing to do harm to the company.

An employee working with an outside entity to attack the company.

I put this as a major threat that is still possible because I’m sure there have been attacks planned out and executed this way, but the amount of time and effort put into getting the person in place will likely outweigh the benefit of doing so. Any company who runs a more likely risk of this happening will already have a screening process in place to prevent them from getting hired. If they were to get through all that, however, this would be a major threat to the company to have someone on the inside who wishes to do harm.

Neutral

Employee missing work.

I was drawing a bit of a blank on this one, but I think that the employee missing work can maybe have very limited consequences when it comes to the security of the company. There can be a bit of information lost or possible missing some meeting where some new policy is discussed but I think this is so rare and unlikely that is negligible.