# Elevation of Privilege Attacks

Riordan Manufacturing has many attack vectors to address across their environment. One class of issues is the elevation of privilege (EoP) attacks. An Elevation of Privilege is when an attacker is able to bypass or gain access to a resource that they would typically not be allowed to use or used in such a manner.

An example of an EoP might be a vulnerability in a web server, once exploited an attacker would have the ability to do anything the web server was able to do. This could include access to middle tier systems behind the firewall, databases, or other high value targets.

Another example might not be a vulnerability but a poor configuration and isolation deployment. For instance if the team web server is also the team certificate authority, and team members can run code on that web server; then those same team members can likely generate certificates. This needs to be mitigated through proper isolation and separation or roles.

EoP attacks are not limited to only vulnerabilities in software they can also exist in the physical realm. An example might be a server room that is not locked or protected by a weak lock. If the attacker is able to gain access to the server room, they can then steal or modify business critical systems and data.

A fourth example might be a random employee does not lock their workstation before leaving for the restroom. If an attacker would to notice this they could jump on the unlocked workstation and perform any action under the context of that random employee. This could allow for bypass of authentication or authorization policy.