YOUR Company logo here

Combined Security Risk Matrix
{Threat + Vulnerability = Risk}
Authored By {VNA}

Prior to Risk Mitigation Strategy				Post Risk Mitigation Strategy		
Threat to Site	**Vulnerability Description**	**Impact of Risk**	**Probability of Occurrence (Almost Certain, Likely, Possible, Unlikely, Rare)**	**Risk Mitigation**	**Impact of Loss Description**	**Probability of Occurrence (Almost Certain, Likely, Possible, Unlikely, Rare)**
Any Town USA						
PH-Criminal Threat - Burglary	no fence, windows surrounding the facility, minimal external cameras	Loss of equipment (monitors, laptops phones), or sensitive proprietary information	Possible	Install motion detection sensors, monitored alarm system and additional cameras	Instillation of motion sensors would activate an audible alarm and act as a deterrent. Actively monitored alarms notify local authorities who respond to the site. Additional external cameras act as a deterrent and provide a tool for identifying involved parties	Unlikely
PH- Natural Disasters - Fires	Outdated or ineffective strobes and alarms, lapse in sprinkler inspections, no regularly scheduled training	Loss of critical scientific assets, loss of equipment, loss of life	possible	Install, repair or replace sprinkler systems, alarms and strobes as needed and include regular maintenance of these systems, provide annual training	Regularly inspected sprinkler system would minimize loss, updated alarms and strobes provide warnings to personnel in the building, and training provides personnel with the knowledge to safely exit the facility.	Unlikely
IT- Industrial Espionage- Electronic Data (outside-in network-based attack)	Internet connected site, traveling workforce, network connected research equipment, potential bad-actor target	Loss of IP, damage to product, interference with business operations, loss of integrity/trust	Likely	Maintain physical and electronic protections; maintain data backup systems; utilize network intrusion detection/prevention systems; monitor, analyze, and safeguard log data; train and retrain employees on evolving IT security awareness	Any damage will be minimal and compartmentalized	Rare
IT - Exfiltration of electronic data/media	Endpoints not physically secured, use of USB mass storage, optical media, etc. is enabled, employees have access to internet-based mail and social media sites.	Loss of IP, compromise of product, interference with business operations, loss of integrity/trust	Possible	Policies, user education, electronic controls, encryption, need-to-know principle, data is primarily stored on centralized servers	Decreased likelihood of undetected exfiltration of data	Unlikely