Parking lot USB exercise

Contents	The contents of the drive found in the parking lot involve various forms of PII (family photos, pet photos) as well as corporate information such as employee work schedules and employee budgets.
Attacker mindset	Information contained in the device may be leveraged against Jorge, or employees of the organization. Employee schedules can be used to strengthen phishing attacks against workers at the organization, or photographs could be utilized to impersonate Jorge.
Risk analysis	An executable file could be placed on the drive that may infect company assets with viruses, malware, or trojans, amongst various other malware. Utilizing antivirus software, having backups of company assets, and continued employee training may mitigate this type of risk and stop a malicious actor before they can find an attack vector.