Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. There are files that contain Jorge Bailey's PII, such as his resume, family photos, and dog pictures. Additionally, there are sensitive work files on the USB drive, such as shift schedules, new hire letters, and employee budgets. It is not safe to store personal files with work files because if a malicious actor gains access to one's device, not only will personal PII be leaked, but also the company's files. Furthermore, a malicious actor may use personal files to impersonate the individual and target others.
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. The information stored on the USB flash drive could potentially be used against other employees, such as Jorge's supervisor. A malicious actor may impersonate Jorge to obtain more information from his supervisor or even deceive the supervisor into granting additional access. Additionally, the information could be used against relatives, as it includes family photos, dog photos, and even a wedding list. A malicious actor could exploit this information to gain trust from relatives and then request money or engage in other deceptive activities. Furthermore, the information stored on the USB drive could provide access to the business. For instance, shift schedules are included, which could be used by a malicious actor to gain physical access to the company. For example, one could use the new hire letter to pose as a new employee and utilize the shift schedules to identify opportune times to physically enter the company.

Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: Operational control, such as promoting employees' security awareness, is crucial since human vulnerability represents the biggest cybersecurity threat. If employees are cautious enough to report any security incidents promptly in the future, the impact on the company could be minimized. Therefore, regular security awareness training sessions are necessary. Technical controls, such as having malware protection, IPS, firewall, and scanning tools in place, could prevent the spread of malware or even stop incidents from occurring. Managerial control, like implementing certain company policies regarding such issues or conducting tabletop exercises beforehand, is also essential. Trojan or ransomware could be hidden inside USB to either open a backdoor or lock data to request ransom. If the device were discovered by another employee, they might simply plug it into the computer. The Trojan contained in the USB could then spread across the company's network, providing malicious actors with more options to request ransom or disclose proprietary information. A threat actor could access personal information such as the owner of the device, the owner's PII, or sensitive company information. This information could be used to threaten to release any company PII if a ransom is not paid.