# Parking lot USB exercise

| | |
|---|---|
| **Contents** | The USB drive contains a mix of personal and work-related files, including family and pet photos, a new hire letter, and an employee shift schedule. This indicates that the drive holds personally identifiable information (PII) and sensitive organizational data that could be valuable if accessed by unauthorized individuals. |
| **Attacker mindset** | An attacker could exploit the personal information to target Jorge Bailey with social engineering attacks or phishing scams. The work-related documents, such as the new hire letter and employee shift schedule, could be used to compromise the hospital's operations or to gain further access to internal systems by impersonating employees or manipulating schedules. |
| **Risk analysis** | USB baiting attacks pose significant risks as they can deliver malicious software such as ransomware, keyloggers, or backdoor Trojans. If another employee discovered and used the infected USB drive, it could lead to data breaches, system compromises, and operational disruptions. To mitigate these risks, implementing technical controls like endpoint security software, enforcing operational controls such as regular employee training on safe USB practices, and establishing managerial policies for handling found devices and reporting suspicious activities are essential. Additionally, using network segmentation and access controls can limit the impact of any potential compromise. |