Attack Vectors – Portfolio Activity

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. • These files may contain personally identifiable information (PII) such as names, contact information, and employment details. • Storing personal files alongside sensitive work documents on a USB drive is unsafe and increases the risk of data leakage.
Attacker mindset	• An attacker could use the personal and HR-related files to craft targeted phishing emails or impersonate Jorge to gain trust and access. • Information about shift schedules and new hires could be used to plan social engineering attacks against other employees. • The entire USB drive may have been staged to lure someone into plugging it in, potentially opening a backdoor into the hospital's network.
Risk analysis	• USB baiting attacks can deliver malicious software such as ransomware, spyware, or keyloggers that compromise systems or steal data. • If another employee had found and plugged in the infected USB, it could have jeopardized the hospital's systems and patient data • A threat actor could extract sensitive employee or operational data and exploit it for identity theft or network intrusion. • To mitigate these risks, organizations should enforce USB use policies, provide cybersecurity awareness training, implement endpoint protection, and restrict USB ports through device control software.