Parking lot USB exercise

Contents	• Files contain personal as well as work-related information • PII and business-related confidential information is also present. • Personal information related to family and plans is also available
Attacker mindset	• Resume and shift schedules can be used to target specific employees. • Employee budget and new hire letter documents can be used for social engineering to get money or impersonate a new hire • Vacation ideas with family photos can be used to target family members in phishing or vishing attempts
Risk analysis	• *There could be malware such as spyware, rootkits or ransomware payloads in this drive, by preventing autoplay on company PCs can prevent code execution when a USB is plugged in* • *PII, confidential and any information that can gain an advantage to go into the network or the business. Providing employee awareness about types of attacks can prevent employees from using USB as a transportation method for information/Data* • *Using phishing attacks, to get employees to give confidential information, install software on their devices by impersonating a different employee etc* • *Running regular virus scans.*