Parking lot USB exercise

Contents	It seems that Jorge has a mixture of both personal and work information stored in this drive. There is a folder containing personal photos and there is also information on a new employee hire letter. In the USB we can see work schedules as well as vacation ideas.
Attacker mindset	An attacker can use this information to alter employee work schedules. An attacker can also rewrite and leak the hire letter including sensitive information or even adding or subtracting pay. The attacker could choose to leak and distribute Jorges pictures throughout the company.
Risk analysis	This USB device could have had malicious code stored in it which can create a backdoor access to the company. The drive could have also had spyware that coil continuously monitors the hospitals network and database. An attacker could have decided to leak private information belonging to Jorge, PII belonging to the new hire and employee information that is related to scheduling.