Parking lot USB exercise

Contents	Information contained on the USB stick is several instances of PII. Budget information and scheduling information looks to be the most sensitive company information stored. Work and personal files should NOT be stored on the same storage device to prevent leaking of sensitive company data to unknown and unverified sources.
Attacker mindset	Information such as the schedule stored on the USB stick can be used by threat actors to track down employees. Other information on the drive exposes Jorge himself with wedding and vacation ideas and plans, threat actors could take advantage and launch phishing attacks. The budget information on the USB stick could also compromise business operations due to sensitive financial information being leaked to a potentially unknown source.
Risk analysis	An unknown USB drive could contain a virus, malware, or spyware that could be installed onto an unsuspecting employees workstation. The different types on sensitive information that can be found on devices like this can range from personal finances, schedules, and location information and business plans, marketing information, employee information, and corporate finances. All these types of information can be used to impact personal and business functions of the victim/employee by leaking or selling information to the public. Making sure employees are aware of how to handle and approach situations like this are important to reduce the attack surface of threat actors.