Parking lot USB exercise

Contents	• *Jorge has stored both private and business files at one place which definitely contains personal identifiable information.* • *There are multiple sensitive files which contain managerial and financial data.* • *It is not at all safe to keep the personal data and work files together.*
Attacker mindset	• *The information found on the usb is a PII and can be used against the employee who is hired and his offer letter is in the usb.* • *The files in usb reveal too much about the personal life of Jorge, this information can be used against his relatives too.* • *No, the usb does not contain any type of credentials which can be used to access the organization.*
Risk analysis	• *These devices may contain viruses such as Trojan Horse which can multiply and hide itself. If the device was infected and another employee has used it on the system, it would have resulted in a serious risk which may lead to data leakage and other major risks.* • *Sensitive information like PII of Jorge, employee budget of organization, an employee's offer letter, employee's schedule etc.* • *This information may be used by an attacker to define which employee is at work on what time, they can gather information about Jorge's private life. The organizational budget is an important and sensitive file which can result in financial harm to the organization.* • *Promoting employee awareness about these types of attacks and what to do when a suspicious USB drive is a managerial control that can reduce the risk of a negative incident. Setting up routine antivirus scans is an operational control that can be implemented. Another line of defense could be a technical control, like disabling AutoPlay on company PCs that will prevent a computer from automatically executing malicious code when a USB drive is plugged in.*