Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *Are there files that can contain PII?* *Yes, there are files such as a hire letter, a job resume, family and pet photographs and a wedding list that can contain PII (personally identifiable information)* ● *Are there sensitive work files?* *Yes, Employee budgets and shift schedules are sensitive work files that are confidential to the organization.* ● *Is it safe to store personal files with work files?* *No, I think it isn't safe to store personal files with work files, as personal files may interfere with an organization's integrity of work data, leading to potential data losses. Also, work files often need to be accessed by multiple colleagues, and mixing them with personal files can lead to unauthorized access to private information.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *Could the information be used against other employees?* *Yes, since the USB drive contains information about employee budgets and shift schedules, this information can be used by a threat actor to impersonate an employee and gain unauthorized access to the company's data and may exploit any vulnerabilities.* ● *Could the information be used against relatives?* *Yes, one of the files in the USB device is a wedding guest list, which can potentially contain personal information about friends and relatives such as their names, contact details and even addresses which can be misused by threat actors. This also contains family and pet photographs which can be used in dangerous ways, an example being deepfake.* ● *Could the information provide access to the business?* *The hire letter may contain any login instructions and may mention access to certain information in the company, which may give off any information or access to the business.*

Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* *The photographs may have been embedded with any malicious software that could affect the system when opened or downloaded. The vacation travel ideas may contain links to malicious and non reputed websites which may obtain PII from visitors or even redirect them to install any malicious software.* ● *What sensitive information could a threat actor find on a device like this?* *The hire letter, shift schedules, employee budgets and photographs can be exploited by a threat actor, if found.* ● *How might that information be used against an individual or an organization?* *The photographs are PII and may be used to blackmail the individual, or even may land up in malicious sites as deep fakes. The shift schedules and the employee budgets can be used to gather information to impersonate and employee and try to gain unauthorized access into the company's system, which can later lead to deletion, sharing or even stealing valuable company data.*