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?* ● *Are there sensitive work files?* ● *Is it safe to store personal files with work files?* *According to the information given there are sensitivity files within the USB like family photos, and wedding files. The USB does contain sensitive files like employees' budgets and a letter to the new hire which can contain private content. It is not safe to store work and personal files together because the personal files will be more at risk if lost or stolen.*
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?* ● *Could the information be used against relatives?* ● *Could the information provide access to the business?* *The information can affect the other employees because the data can be used to access private information. The information can be used against relatives because people can find out who they are and go to the location of the wedding which can be dangerous for them. The information can also provide access to the attacker since they can see the employee's shift schedule and their budget which can be modified.*
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?* ● *What sensitive information could a threat actor find on a device like this?* ● *How might that information be used against an individual or an organization?* *Some types of malicious software can be a viruses that can take control of your computer to do certain things that you as a user won't do. Ways to prevent this risk is by creating awareness of this risk like phishing emails and ensuring employees know what to do and how to report the issue. If a computer is compromised*

	it will be better to take it offline and be dealt with immediately to ensure no company data gets compromised and mediate the effects of the attacks