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?* *The USB drive discovered in the parking lot contains a blend of personal and work-related files attributed to Jorge Bailey. Among these files are family and pet photos, a new hire letter, an employee shift schedule, and documents containing personal information that Jorge wouldn't want to be made public. The work-related files include personally identifiable information (PII) of other individuals and sensitive information regarding the hospital's operations. The mix of personal and work data on the same device poses a security risk and shows the importance of keeping the information segregated.*
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 timesheets found on the USB drive could provide an attacker with valuable information about Jorge's coworkers, potentially giving them the ability to impersonate a colleague or family member in a malicious email. The combination of personal and work files on the device creates an opportunity for attackers to craft convincing phishing emails or gain insights into the hospital's operations. This poses risks such as unauthorized system access, data breaches, and targeted attacks against Jorge or other hospital staff members.*
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?* *Implementing a comprehensive strategy to mitigate USB-baiting attacks involves multiple layers of control. Employee awareness training to educate staff about these threats and how to respond*

	to suspicious USB drives effectively. Operational controls, like routine antivirus scans. Additionally, technical controls like endpoint security software with USB scanning capabilities and disabling AutoPlay on company PCs can help strengthen protection against malicious code from executing from USB drives. Combining these security measures reduces the risk of unauthorized access and potential data breaches.