Parking lot USB exercise

Contents	There are several files on the device that contain Jorge's personally identifiable information (PII), such as a wedding guest list, family details, and other private data. In addition, there are sensitive work files like shift schedules, meeting summaries, and employee budget records. It is not safe to store personal files with work files because combining them increases the risk of data breaches. Keeping them separate helps protect both personal and professional information.
Attacker mindset	This information could be used against Jorge or the hospital by threat actors to impersonate, manipulate, or blackmail them, or to access internal systems. It could also be used to target other employees, especially if work-related data is altered or leaked. Since the hard drive contains family information, relatives could be at risk too, and sensitive business data could provide unauthorized access to hospital systems.
Risk analysis	Malicious software like ransomware, spyware, or keyloggers could be hidden on the hard drive and executed once connected to a personal or business computer, potentially leading to data loss or unauthorized access. If another employee discovered the infection, it could damage trust, expose sensitive data, or disrupt operations. To mitigate these risks, technical controls such as USB device scanning, antivirus software, and network segmentation should be implemented. Operational and managerial controls like employee cybersecurity awareness training, strict data classification policies, and limited access to sensitive information help reduce the likelihood and impact of such attacks.