Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. *The USB drive contains a mixture of personal and work-related files, including Personally Identifiable Information (PII) such as Jorge Bailey's details and employee records from Rhetorical Hospital. In addition to sensitive employee data, the USB also holds work-related documents concerning the hospital's internal operations. Storing personal files alongside work files, especially ones containing sensitive information, is not safe as it increases the risk of data exposure and potential exploitation of both personal and business-related data.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. *The timesheets and other sensitive files on the USB drive could provide an attacker with valuable details about Jorge and his colleagues, including work schedules and personal information. This data could be exploited to craft convincing phishing emails or social engineering attacks, targeting both Jorge and other employees. Additionally, the information could be used to impersonate coworkers or relatives, further compromising the security of Jorge, his colleagues, and potentially even gaining unauthorized access to the hospital's systems.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: *Promoting employee awareness and conducting regular security training on identifying and handling suspicious devices are essential managerial controls that can mitigate the risk of malicious USB drives. Operational controls, such as enforcing routine antivirus scans and monitoring the use of removable media, help identify threats before they escalate. Implementing technical controls, like disabling Autorun on all company PCs, prevents the automatic execution of malicious code when a USB device is connected. If a device were infected, it could spread malware, such as keyloggers or ransomware, potentially leading to unauthorized access to sensitive hospital information, including PII, financial records, or even confidential medical data. A threat actor could leverage this information to launch phishing attacks, compromise employee credentials, or disrupt hospital operations.*