Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● Some of the files found on the usb drive contain PII about an HR representative that works at the company. ● There are also sensitive files about new hires and employee budgets. ● The CISA states that best practice when it comes to USB drives is to keep work and personal related drive contents separate from each other.
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● Since the drive contained employee budget information and shift schedules this information could have been leaked to employees early causing confusion. ● The information contained in the drive also had PII of individuals not particularly involved with the company which could have been used in malicious ways. ● Depending on password policy and security posture already present at the company the information contained in the drive could provide a basis to perform a malicious brute force attack or other network breaching attack.
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● USB drives found could have been stolen by a malicious actor and loaded with malware or system hijacking code that may have compromised a potentially vital system. ● A threat actor could have found the PII or SPII of employees or outside parties. ● The PII/SPII of individuals gleaned from devices like this could be used to stage a future attack. Such as gaining unauthorized access to a sensitive database or blackmailing an employee for more company secrets.