Parking lot USB exercise

Contents	• On Jorge Bailey's USB drive, there is a mix of personal and work-related files. Personal files include family and pet photos, while work-related files consist of a new hire letter and an employee shift schedule. This combination of data suggests that Jorge has stored both personal and work-related information on this device, potentially mixing sensitive personal files with professional ones.
Attacker mindset	• The information found on the USB drive could be used against Jorge or the hospital in several ways. If the event was staged by an attacker, they might have strategically mixed personal and work-related files to create a sense of authenticity and lure Jorge or another employee into connecting the USB drive. Once inserted into a workstation, this could trigger a malicious payload or establish a backdoor into the hospital's systems. Additionally, the personal files could be exploited for social engineering attacks against Jorge or his colleagues, potentially leading to identity theft or phishing incidents targeting hospital employees.

Risk analysis	● USB baiting attacks can pose significant risks, even without containing malicious software. If the device were infected and discovered by another employee, it could lead to the unintentional spread of malware within the organization, potentially compromising sensitive data or disrupting operations. Threat actors could find a wealth of sensitive information on a device like this, including personally identifiable information (PII) and work-related files. This information could be exploited for identity theft, spear-phishing campaigns, or gaining unauthorized access to the organization's systems. To mitigate USB baiting attacks, organizations should implement a combination of technical controls like endpoint security software, operational controls such as user awareness training, and managerial controls like strict policies on the use of external storage devices.