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 following files in the USB contain PII: Family photos, Wedding list, JB_Resume. These files contain visual personal identifiers, names, phone numbers, e-mail addresses, and possibly home addresses. There are also sensitive work files like the New hire letter, the Employee budget, and Shift schedules. Generally, it isn;t safe to store personal files with work files, as personal files should never become part of a business' database if they have nothing to do with overall operations.
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 Shift schedules file can pose a serious physical security threat to any of the listed individuals, since it would let a threat actor know when anyone will be physically present at the hospital. This can leave employees vulnerable to anyone wanting to conduct any malicious crime against them. The Wedding list contains the names of relatives, who can then be targeted somehow for blackmail against Jorge Bailey, and potential harm can come their way via something like ransom. The Vacation ideas document may give a threat actor a hint as to when a large group of individuals from the hospital will be absent and not active, therefore, giving a threat actor an idea of when the business may be vulnerable to cyber-attaacks, since the workforce will be weakened.

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?* This USB could have contained a computer virus that could potentially run a program that could severely impact the hospital's network through malicious code that can alter files and programs that are crucial to business operations. There could also be ransomware, or Trojan viruses on the USB. A threat actor can use the photos of family members to create threats to the USB's original owner, giving a sense of danger to loved ones, and demanding some sort of ransom. A threat actor can also use the Employee schedule to target employees at their physical location. The individuals and organization can be in danger of violent terrorist acts if a threat actor can discover their exact locations on any given day. To mitigate such tasks, the USB can be outfitted with some form of password unlock mechanism such as dual-factor authentication any time it is connected to a device. Another control is implementing a lock on the Excel documents with employee information, so that it becomes a shared document, with only authorized password-holders given the ability to read the documents. The owner of the USB could have also used separate USBs for personal and business purposes, to avoid mixing their personal life and sensitive business documentation. It may also be advisable to store the business-related documents on the company's server, rather than a physical USB which has a greater chance of falling into the wrong hands, since the company's network is more likely to have strict security measures in place than an external memory drive.