## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | Write **2-3 sentences** about the types of information found on this device.  The USB drive contains a mix of personal and work-related files belonging to Jorge Bailey, the human resource manager at the Rhetorical Hospital. The personal files include family and pet photos, while the work-related files include a new hire letter and an employee shift schedule. This combination of personal identifiable information (PII) and sensitive work documents poses a significant security risk. |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.  An attacker could exploit the information on the USB drive by using the PII to target Jorge or his relatives through phishing or social engineering attacks. The work-related files could provide the attacker with valuable insights into the hospital’s operations, potentially leading to more sophisticated attacks, such as spear-phishing emails to employees or attempts to infiltrate the hospital’s network. |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:  USB baiting attacks can hide various types of malicious software such as keyloggers, ransomware, or remote access Trojans (RATs). If the device were infected and another employee plugged it in, it could compromise the hospital’s entire network. Sensitive information found on the device, like employee schedules and new hire details, could be used for identity theft or to plan further attacks. Mitigation strategies include implementing strict policies against using unknown USB drives, using endpoint security software to scan all external devices, and conducting regular cybersecurity training for employees to recognize and report suspicious devices. |