## **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 USB drive contained PII such as family and pet photos, sensitive work files such as new hire letter and employee shift schedule. It is absolutely not safe to store work and personal files together. |
| **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 attacker could use Jorge’s PII photos to impersonate and manipulate his relatives. The attacker could also use the timesheets to better understand those that work with Jorge. |
| **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?*   There could have been a malicious malware that when connected to a device, it would install unwanted viruses and ultimately disrupt the entirety of the company. A threat actor could find vulnerabilities or exploits in USB’s such as these. If an attacker were to gain sensitive information from a USB such as this, if they were skilled enough they could implement a number of attacks, from vishing, infecting malware, or a brute force attack to gain access to the companies sensitive data. |