## **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?*   Yes, several files contain PII like Jorge’s family pictures and the date Jorge is getting married. There are also sensitive work files like shift schedule information and employee budgets, which are also PII of other employees.  It is not safe to store personal files with work files. For example, some users use important dates (like their wedding date) as their password to access the system. There is also sensitive data about the company’s 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 information could be used against other employees. For example, the employee budget could be used for blackmail or to cause another employee to be disgruntled as they are being underpaid. The information could also be used against Jorge as blackmail to get him to release confidential business information.  The information could also be used against Jorge’s relatives. |
| **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?*   If the device was infected and discovered by another employee, the USB could have installed malware into the system and spread it across the network. The information found in the device could be used for blackmail, or could inform a brute force attack to get into the systems.  Promoting employee awareness about these attacks is a good managerial control to prevent people plugging in USB sticks. From a security standpoint, computers could also be set-up so they do not accept flash drives unless it’s in a virtual system. Disabling AutoPlay on computers will also prevent USBs from automatically executing malicious code. |