## **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? Yes, there are files that contain PII. There is a new hire document in the USB drive.* * *Are there sensitive work files? Yes, there is a new hire file and an employee budget worksheet.* * *Is it safe to store personal files with work files? It is never safe to store personal files and work files together. It is far too easy to accidentally share classified information from work files.* |
| --- | --- |
| **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? Yes, someone could find out who is working what shifts to learn their schedules.* * *Could the information be used against relatives? Yes, there is a wedding list that could include relatives’ names and information.* * *Could the information provide access to the business? Not directly, but a threat actor could use this information to gain access to the business by using other means.* |
| **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? There could be a worm on it that could upload itself to another person’s device without being detected.* * *What sensitive information could a threat actor find on a device like this? They could find PII of an individual or sensitive information about the company.* * *How might that information be used against an individual or an organization? A threat actor could hold this information for ransom while threatening to release files to the public unless they are paid a certain amount of money.* |