## **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 found does in fact contain PII as it contains a wedding list for Wendy & Jorge. There is also sensitive work information such as employee budget and shift schedules. It is not a good idea to store both personal files and work files together, it is much better to store them separately each with there own set of security polices and access rights to limit who sees the information.*** |
| **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 schedule is indeed something that can be used against the business or other employes as it gives threat actors information about who is working and when. The wedding list can be used as potential threat to relatives as they often include family names and possible address locations if the wedding invitation information is apart of the list.*** |
| **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?*   ***Finding a USB on the ground even if it wasn’t meant to be a malicious act could still carry unknown malware and/or other malicious software they could be malicious in nature and a threat to the business. It is best to not allow outside devices to be used without proper inspection and scanning as to prevent accidental damage of company assets and/or unknowingly giving an outside threat potential entry. As shown from the example above it is very possible to find PII, or other company assets if they have not been stored and encrypted properly.*** |