## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | Write **2-3 sentences** about the types of information found on this device.  The USB belongs to Jorge. The contents contained a mixture of personal and work-related files. It included family photos, several other personal files and the work files include the PII of other people and information on the hospital’s operations. This is poor practice since it is not good to store personal files with work files. |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.  The personal files can be used to trick Jorge through social engineering and the work files such as the work shift schedule can provide an attacker with information about the people Jorge works with. |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:  To mitigate these types of attacks, several technical, operational, and managerial controls can be implemented. Technical controls, such as disabling USB ports or using endpoint protection software, can prevent unauthorized devices from being connected and block malicious software from executing. Operational controls, like enforcing routine device checks and regular software updates, ensure systems remain secure against potential vulnerabilities. Managerial controls, including employee training programs to recognize and report suspicious devices, enhance awareness and reduce the likelihood of an incident. Additionally, implementing a policy requiring encrypted USB drives for business use can protect sensitive information if a device is lost or compromised. |