# Parking lot USB exercise

| | |
|---|---|
| **Contents** | Write **2-3 sentences** about the types of information found on this device.<br><br>Some documents appear to contain personal information that Jorge wouldn't want to be made public. The work files include the PII of other people. Also, the work files contain information about the hospital's operations. |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.<br><br>Timesheets could potentially expose Jorge's coworkers' or relatives' information to attackers, which could then be used to deceive Jorge. For instance, attackers could craft a malicious email to appear as if it were from someone Jorge knows, using either work-related or personal information gleaned from the timesheets. |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:<br><br>Educating employees about such attacks and providing guidance on handling suspicious USB drives is a managerial measure that can mitigate the risk of a harmful incident. Conducting regular antivirus scans is an operational measure that can also be enforced. Additionally, a technical measure, such as disabling AutoPlay on company PCs, can serve as another layer of defense, preventing the automatic execution of malicious code when a USB drive is inserted. |