## **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 is a resume as well some family/pet photos. Other documents listed are Vacation Ideas, and Wedding List,* * *Are there sensitive work files?*   + *Listed files in the DRIVE show that there is an EMPLOYEE Budget Tracker, Shift Schedule at Workplace, and a RESUME, which truly seems work related* * *Is it safe to store personal files with work files?*   + *They should be separated. Especially work files mixed with Personal Photos is not permitted. Work place files should be kept at work. To bring home work if necessary must be kept confidential with other security controls in place such as Encryption, MFA, and VPN.* |
| --- | --- |
| **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?*   + *The work information shown as well as the PII truly reveal enough information for the the threat actor to perform identity theft and using this information against the individual can provide an attack vector and can easily manipulate Jorge.* * *Could the information be used against relatives?*   + *Yes, same as employees. Personal information even during their leisurely time can compromise them whether they are at work or not. Jorge can easily be tricked.* * *Could the information provide access to the business?*   + *The new hire letter, employee budget tracking, resume, and employee schedule are good starting points for the threat actor to work with. This can truly be enough for reconnaissance and information gathering* |
| **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?*   + *BadUSB Script designed to steal a user’s information or perhaps infect an organization’s network. Never can tell, but so many possibilities. Malicious script designed to infect a user’s computer or infect a network.* * *What sensitive information could a threat actor find on a device like this?*   + *Computer Memory, Passwords, Encryption Keys, and other various sensitive data*   + *Technical Controls should be in place.* * *How might that information be used against an individual or an organization?*   + *Depending on the information that was stolen especially medical records this would violate HIPPA and the threat actor could use this to their advantage for illicit purposes such as identity theft.* |