## **Parking lot USB exercise**

| **Contents** | Write **2-3 sentences** about the types of information found on this device.   * *Three files that contain PII are New Hire Letter, JB\_Resume, and Wedding List.* * *The sensitive work files are the Shift Schedules, and Employee budget files.* * *Personal files should be separated from work files for the protection of PII and Employee PII incase of the flash drive being compromised you mitigate the risk of both categories of information being misused all together.* |
| --- | --- |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.   * *Having the work files, the threat actor could possibly impersonate one of the employees using their credentials.* * *Having the relatives' information could set them up for threat actors to sell their information in the dark web which could then open up doors for the family to receive countless phishing attempts, vishing attempts, to gather possible information to be used in identity theft.* * *The work information could provide access to the company, because the threat actor knows the employee schedule and could plan an attack to infiltrate the company further through a physical attack or digital attack after work hours.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:   * *Promoting employee awareness of these types of attacks and what to do when you find a USB drive.* * *Configure an antivirus software to perform frequent virus scans.* * *Disable Autoplay on company PCs to prevent a USB drive from automatically opening files when the USB drive is plugged in.* |