## **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?*   *There are family pictures and pictures of the person’s dogs. Also, the drive has his resume which has his address.*   * *Are there sensitive work files?*   *The drive also contains files such as, “Employee budget” and “Shift schedule”*   * *Is it safe to store personal files with work files?*   *No, it is not safe to store personal and work files because if both are together on the same drive then, if the drive is lost or stolen, anyone malicious would have access to both. As if they hit 2 birds with one stone.* |
| **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?*   *Maybe from the employee budget file it could list the salaries of employees and an attacker could maybe exploit them. For example, if someone doesn’t make as much they probably wouldn’t be an enticing target.*   * *Could the information be used against relatives?*   *Other than the address that is listed on the victim’s resume and the family photos, there isn’t too much information that could be used against relatives.*   * *Could the information provide access to the business?*   *Yes the shift schedules may provide access to the business since one could impersonate an employee since they would know who starts at what time exactly.* |
| **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?*   *Trojan horses, backdoors, just plain viruses which all could cause damage to a hospital and may even endanger patients. Even a spear-phishing attack could be conducted against Jorge because the attacker would have some information that would generally be only known to the organization from the organization. If the device was actually infected and was picked up by a non-technical person and had just inserted, it into their work computer then they could’ve inadvertently compromised the whole hospital. Especially if this device wasn’t used in a sandbox.*   * *What sensitive information could a threat actor find on a device like this?*   *Personal and work files that could be used to exploit the actual employee or an attacked could social engineer their way into the actual organization itself.* |