## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | The files on this device contain sensitive work documents such as an employee shift schedule, as well as PII such as a new hire letter that may contain emails and addresses. If this USB only contained the family and pet photographs, the impact that would be made by leaving this USB around would be minimized drastically. |
| **Attacker mindset** | The information on this USB can be used against Jorge or the hospital he works at. For example, the JB\_Resume.gdoc file may contain Jorge’s personal information and could be used to impersonate him. Additionally, this could lead to accessing sensitive documents from the hospital if there are names or email addresses in the Shift schedules.gsheets file or leak private financial information found in the Employee budget.gsheets file. |
| **Risk analysis** | If this USB was infected and used by another employee, the resulting damage could be catastrophic to the business. If an attacker found this USB with company emails, names, financial information, or patient records, they could be able to exploit that and access the internal network of the company.  An example of using operational controls would be to brief employees on media protection and training them in the risks of leaving sensitive information on portable storage media. Storing these sensitive files in a database that is protected by the company is a much more secure way of storing this data. |