## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | The USB drive contains both personal and work-related files which include family photos, a new hire letter, and a work shift schedule. Some of these documents contain sensitive information such as PII. |
| **Attacker mindset** | There is a budget document and work schedule which identifies other people at the company which an attacker may use for identity theft. Exposure to the public of internal information may damage the company’s reputation. One or more of the files may contain malware and create a backdoor should someone try opening the files. |
| **Risk analysis** | The company may enforce managerial controls such as adding password protection to internal files or restricting permissions on the files themselves or by using access control. Operational controls may include educating employees on the risks of USB baiting and to not open any files found on a drive to prevent malware attacks. |