## **Parking lot USB exercise**

| **Contents** | In the drive were found both work-related and personal data, including files that contain the employee’s PII and others that contained sensitive work files. Maintaining personal and work related files on the same drive is dangerous, and company policy should prohibit this practice. |
| --- | --- |
| **Attacker mindset** | The data in the drive could be used as a source of internal-only intelligence for an attacker;  An attacker could use information like the new hire letter to target the newly hired employee that may lack proper security training; the shift schedules to know when the fewest employees are working to conduct physical attacks; and the employee budget report to harm the business.  The personal information could also be used for blackmailing or crafting spear phishing emails to the employee in question. |
| **Risk analysis** | Based on this analysis, the SOC recommends the following controls:   1. Stricter policies about saving personal data on work related systems (workstations, laptops, drives, cloud storage) 2. All work-related data must be stored in corporate cloud stored drives, such as Google Drive. |