## **Parking lot USB exercise**

| **Contents** | Inside the drive, there’s a mix of personal and work-related files. Jorge’s resume and shift schedule is in there. I personally would not recommend storing personal files with work files as it’s not safe when you lose both. |
| --- | --- |
| **Attacker mindset** | An attacker could have placed these files on the USB drive as a distraction. They might have targeted Jorge or someone he knows, hoping they would find the device and plug it into their workstation. In doing so, the attacker could establish a backdoor into the company's systems while the unsuspecting target browsed through the files. |
| **Risk analysis** | Promoting employee awareness about these types of attacks  and what to do when a suspicious USB drive is a managerial  control that can reduce the risk of a negative incident. Setting up  routine antivirus scans is an operational control that can be  implemented. Another line of defense could be a technical  control, like disabling AutoPlay on company PCs that will prevent  a computer from automatically executing malicious code when a  USB drive is plugged in. |