## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | information found on this device.  *Some documents appear to contain personal information that Jorge wouldn’t want to be made public. The work files include the PII of other people.* |
| **Attacker mindset** | how this information could be used against Jorge or the hospital.  *The timesheets can provide an attacker intel about other people that Jorge works with. Either work or personal information could be used to trick Jorge. For example, a malicious email can be designed to look as though it comes from a coworker or relative.* |
| **Risk analysis** | technical, operational, or managerial controls that could mitigate these types of attacks:  *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.* |