

Parking lot USB exercise

Contents	<p>Write 2-3 sentences about the types of information found on this device.</p> <p><i>There are certain documents that seem to contain private information that Jorge wouldn't want to be shared. The PII of other people is contained in the work files. The job files also include details regarding how the hospital is run.</i></p>
Attacker mindset	<p>Write 2-3 sentences about how this information could be used against Jorge or the hospital.</p> <p><i>The timesheets could give a potential attacker information about other coworkers of Jorge. Jorge could be duped using either professional or personal data. A malicious email, for instance, could be made to appear as though it were sent by a friend or relative.</i></p>
Risk analysis	<p>Write 3 or 4 sentences describing technical, operational, or managerial controls that could mitigate these types of attacks:</p> <p><i>A managerial measure that can lower the probability of a negative incident is promoting staff understanding of these types of assaults and what to do when a suspicious USB drive is discovered. You can create an operational control by setting up regular antivirus scans. Another line of defense could be a technological one, such as turning off AutoPlay on business computers to stop them from running malicious code whenever a USB device is plugged in.</i></p>