

Parking lot USB exercise

Recent

My files

Downloads

Google Drive

My Drive

Jorge's USB

Family photos

Our dog pics ...

Shared drives

Shared with me

Offline

My Drive > Jorge's USB

Folders

Family photos

Our dog pics

Files

New hire letter.gdoc

Vacation ideas.gdoc

Shift schedules.gsh...

Employee budget.g...

Wedding list.gslides

JB_Resume.gdoc

Contents	<i>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. Also, the work files contain information about the hospital's operations.</i>
Attacker mindset	<i>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.</i>
Risk analysis	<i>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.</i>