Parking lot USB exercise

Contents	There is a mix of personal and work files stored on the USB drive. There are personal files such as photos that contain PII. There are also sensitive work files such as shift schedules and employee budgets.
Attacker mindset	This information could be used against Jorge and his family as it contains his PII. The attackers could target members of Jorge's family. The information could also provide attackers with access to the business as they can gain knowledge on when certain employees work. 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	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.