Parking lot USB exercise

Contents	USB drive contains an assortment of personally identifiable information (PII). Attackers can easily use this sensitive information to target the data owner or others around them. Its not safe to store PII data with work files.
Attacker mindset	Timesheets can provide attackers with information about Jorge's colleagues and associates. This work or personal information could be exploited to deceive Jorge. For instance, a malicious email could be crafted to appear as if it is from a coworker or relative.
Risk analysis	Promoting employee awareness about these types of attacks and advising on what to do when encountering a suspicious USB drive is a managerial control that can reduce the risk of negative incidents. Implementing routine antivirus scans serves as an operational control. Another line of defense is a technical control, such as disabling AutoPlay on company PCs, which prevents a computer from automatically executing malicious code when a USB drive is plugged in.