Parking lot USB exercise

Contents	The USB contained both personal and professional documents. Some files included personally identifiable information (PII) related to Jorge's coworkers, while others held sensitive internal data about hospital operations, including schedules and timesheets that were never meant for public access.
Attacker mindset	An attacker could use the PII or workplace details to craft a convincing phishing attack. By mimicking a coworker, vendor, or relative, they could trick Jorge or other staff into clicking malicious links or surrendering credentials. The timesheet data also reveals Jorge's work schedule and colleagues, which could help an attacker time or target an attack.
Risk analysis	To prevent incidents like this, organizations should implement a mix of managerial, operational, and technical controls. - *Managerial: Train employees not to plug in unknown USB drives and report suspicious devices immediately.* - *Operational: Enforce regular antivirus scans and require IT review of any removeable media.* - *Technical: Disable AutoPlay/AutoRun functions on all company devices so no code runs automatically when a drive is inserted.*