Parking lot USB exercise

Contents	Upon investigating, the USB belongs to Jorge Bailey, the human resource manager at Rhetorical Hospital. Jorge's drive contains a mix of personal and work-related files. For personal files, it contains folders that appear to store family and pet photos. As for work-related files, there is a new hire letter, an employee shift schedule and an employee budget tracker. The files that can contain PII is the new hire letter and employee shift schedule. The employee budget tracker is sensitive because it involves financial information. It is not safe to store work and personal information together.
Attacker mindset	This information could be used against the company, other employees as well as against Jorge's family because it involved a mix of work and personal data. Their data could be used for blackmail or social engineering, example an email could be from someone pretending to be Jorge's family member. The employee shift schedule could be an intel for attacker to know employee's movement.
Risk analysis	Raising employee awareness about these types of attacks and educating them on how to handle suspicious USB drives is a crucial managerial control that helps mitigate the risk of security incidents. Regular antivirus scans serve as an essential operational control to detect and remove potential threats. Enforcing technical control such as disabling Autorun/Autoplay is also important to prevent malicious code on an infected USB drive from opening automatically. USB drives pose a significant security risk as they can be used to deliver malware, steal sensitive data, or facilitate unauthorized access to systems. To prevent such threats, organizations should enforce policies restricting the use of unauthorized USB devices, implement endpoint security solutions to monitor and block unapproved external storage, and encourage employees to report any unknown USB drives found in the workplace.