Parking lot USB exercise

Contents	The USB stick contains personal and work-related documents. The USB stick appears to belong to Jorge Bailey, the HR manager at Rhetorical Hospital. There are documents relating to vacation ideas, Jorge's resume, and wedding lists. Also, there are documents that can be harmful if disclosed. They are the employee budget, shift schedules, and new hire letter documents. The work-related files include crucial business information and Personally Identifiable Information (PII) and should be secured as soon as possible. It is not safe for any employee to store work files with personal files.
Attacker mindset	An attacker could use the PII to target the data owner or others around them. This data can be used by an attacked to craft a social engineering attempt toward Jorge. In addition, the attacker could use the contact information for the employees in the files to attempt to attack them as Jorge. Another possible scenario could be if the attacker placed the drive themselves to trick the investigators. Pretending it belonged to Jorge and once plugged into a business computer a program could run to install a virus or worm. If these attacks were successful, it is plausible that the attacker could gain access to the business.
Risk analysis	There are a variety of controls that can mitigate this type of attack. The most important one being the training of employees. If the employee is skeptical and aware of the types of attacks, they would immediately flag the USB as suspicious. Additionally, encrypting company owned USB drives can prevent them from being accessed if they are lost or stolen. Regularly conducting antivirus scans and disallowing USB ports on company workstations can prevent malicious programs from being installed/running from a USB stick. Setting the boot priority to not select USB can also be beneficial in preventing malicious USB sticks from compromising a workstation.