Parking lot USB exercise

Contents	Upon opening the USB in a secure, air-gapped, virtualized environment, the contents show that the USB belonged to an employee named 'Jorge Bailey', a HR manager at the Rhetorical Hospital. ● *Within the USB it is noticed that it contains a mix of personal and work related files. The files with PII are:Vacation Ideas, Wedding List,Family Photos,Dog Pictures, and personal resume.* ● *There appears to be several work-related files within the drive, these include:New hire letter,Shift Schedules,Employee budgets.* ● *It is heavily discouraged to store personal files with workplace files, this opens up many security concerns and is seen as unprofessional.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *This information within the USB can greatly affect not only Mr. Jorge Bailey, but other members of the organization due to the fact that other PII and SPII could possibly be found within the files like: Employee budget shift schedules, letters to new hires. All this information may contain (S)PII on all included employees.* ● *The personal information about Mr.Jorge Bailey may be used to threaten him or any member of his family,blackmail, threats, hacks can be carried out when personal information is leaked or illegitimately gained.* ● *An example of social engineering with Jorge's personal information is that a malicious actor can spoof the email address of a relative based on the gathered information. This makes it much easier to enact a spear phishing attack.* ● *Illegitimate access to the company may be possible through the gathered information though employee communications(New Hire letter or shift schedule) which can provide login information, employee numbers, and login times*

Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *Many forms of malware can be hidden within a USB, these can be: Viruses, Worms, Ransomware(Cryptoware), rootkits, RATs, spyware, etc. All which can be disastrous to a company if given access to a machine and elevated privileges.* ● *An attacker can find everything from PII and SPII to restricted company secretes, any and all information can potentially be used against a individual or a company, causing great harm to all involved* ● *To reduce that chances of a accidental infection of a system via USB is to implementing routine antivirus scans, disabling Autorun, keep personal and business USB separate, and encrypt the data on it.*