Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *Work files, including resumes, and HR related files* ● *There's also some personal files there as well*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *Assuming this is either a legitimate USB stick belonging to Jorge, or simply data with malicious coding on it (with what seems to appear as " valid/legitimate" files).* ● *Someone or Jorge himself may plug it into his PC, thus infecting one or multiple computers, while also creating a backdoor. This would provide an entry point in the company, where files could either be copied and/or deleted.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *Any type of virus could have been included on the USB drive. Perhaps a Lumma stealer or another form of virus that would either steal information and/or register keystrokes. To prevent such a thing from occurring, the USB stick should never be inserted at all. Rather, it should be delivered directly to the Cybersecurity team so they may take the appropriate measures to securely verify the USB in a sandboxed area (and ideally on a VM).*