Parking lot USB exercise

Contents	*There's a shift schedule table from Rhetorical Hospital. Pictures of Jorge's family and PII information on personal files are found like wedding list, vacation travel plans, Jorge's resumé that shouldn't be present on this professional device.*
Attacker mindset	*A threat actor could exploit the information on this USB through social engineering techniques. Personal and professional data allow the attacker to impersonate Jorge, a colleague, or friend to create convincing fake messages, aiming to gain access or perform extortion.*
Risk analysis	*Staff preparation is crucial, as plugging an unknown USB drive into a machine can lead to significant privacy and security breaches. Training should emphasize delivering found devices to security for investigation. Essential controls include using only approved devices, disabling autorun, and maintaining awareness of secure data handling practices.*