Parking lot USB exercise

Contents	There is a combination of personal and work-related files in the USB. The USB belongs to Jorge an employee working in the HR department. The personal and work information should not be stored together as it will increase the attack surface for an attacker to hack more information.
Attacker mindset	The information found in the USB can be manipulated to be used against the hospital, other employees and Jorge. The attacker may have dropped the USB in the parking lot assuming that any employee coming to the hospital would see this USB with the hospital's logo and will plug the USB in his computer out of curiosity. In this way the attacker's motive will be achieved.
Risk analysis	The attacker used the USB baiting technique in order to gain access in the hospital's network system. When any employee will insert the USB in his computer then it will download malicious software which would give access to the hospital's network to the attacker. The information inside the USB can also be used against Jorge as the USB contains his personal information too, the attacker can blackmail him on the basis of his personal info to get the insights of the hospital's private information.