Parking lot USB exercise

Contents	- The contents contain both personal and work files like family pics and employee information. This is dangerous as storing both information in one drive exposes a lot of threat for the malicious actor to exploit.
Attacker mindset	- As an attacker, I can use the information I obtain as a reconnaissance against the company he is working for as I get information about employees shift schedule as well as the employees budget information. I can also exploit the fact that the drive contains an invitation list which includes a lot of invite information like contact or emails which I can then utilize to send phishing mails.
Risk analysis	- If it were a USB baiting attack then employees are risked in curiosity of putting the USB in their devices which might inject malicious malware in their devices. Fortunately it's not but if a malicious actor were to obtain it and use the information expose in the USB then the malicious actor could've exploited all the exposed information in the drive.