Parking lot USB exercise

Contents	There are files which contain assortment of personally identifiable information (PII), such as individual employment details, hire letter, etc. It is not safe to store personal and work files together and it also depends on the policies of the employer to store the data and the sensitivity of the information.
Attacker mindset	The information can be used against other employees because it has new hire letter which can be manipulated and it also has employee shift details which might be beneficial for other rival companies of the employer. The information also includes having wedding list which might be used against relatives. No, the information does provide access to business but it contains employee's shift details which might be helpful to know who works when.
Risk analysis	The USB drive might have potential malwares in it which could be trojan, ransomware, virus, spyware, etc. it might cause data breach, network loss, reputation loss, and even regulation issues such as fines for not protecting PII. The sensitive information a threat actor could find might be either SPII or PII. If those informations are compromised, it might used against individuals in a way where it can cause identity thefts, financial fraud, phishing attacks, etc. For an organization, it might bemused in a way where it might cause data breach, Loss of trust, regulatory and compliance issues.