Parking lot USB exercise

Contents	From observing the drive, the security team found files that contain PII in the USB drive. There is a wedding list that contains dozens of names, potentially related to the owner of the USB drive. More importantly, there is a resume file related to the owner, which can potentially contain addresses, phone numbers, emails, and other information that can tie back to the owner. There are also sensitive work files stored on this USB drive. There is an employee shift schedule, an employee budget tracker, and a new hire letter. All of these can be useful to hackers during their reconnaissance, because they provide information about the company. Storing personal and work files on the same drive is a serious security risk. Work related files should be in a more secure environment than your personal photos and emails. Ideally, you want all things to be secure, but in this case the USB drive should stick to being for work-related matters or personal matters. If it is stolen, the actor will have double the information they would have without.
Attacker mindset	The information found on the USB drive could be used against other employees. Since there is an employee shift schedule and budget tracker, a malicious actor could easily find out information about the business. The information could also be used against relatives of the USB drive owner as well. Since there is plenty of information related to the owner on it. The wedding list potentially has the entire extended family. The information could also provide access to the business for malicious actors. Since there is information on the new hire, a malicious actor can use phishing techniques to easily gain access.
Risk analysis	If the USB drive was infected with malware and discovered by an employee who did not use a VM to access it, the consequences would be severe. Bad USBs (ones infected) typically contain keyloggers or scripts that monitor and steal critical data/information. The data that could potentially leak due to an incident like that would be catastrophic. Depending on the skillset of the attacker, usernames and passwords along with other critically important information could be stolen. A hacker can steal this information by installing a keylogger on the target system when the USB is plugged in. Then all the keys that are pressed on the system are remotely sent to the hacker’s machine, to be used to further access the company’s network.