Jason Ash, Portfolio Exercise

03 Jan, 2026

Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *Are there files that can contain PII?* ○ PII on it could possibly be the shift schedules of employees (this could inform an attacker about shift schedules of security guards or other employees) ○ Contents of the employee budget file ○ The Wedding slides could have photos of people they don't want strangers to see because AI could be used to develop deepfakes. ● *Are there sensitive work files?* ○ The new hire letter could contain Jorge's employee ID and how much that employee makes per hour or per month. ○ Shift schedules could be sensitive work files and other employees might get angry or resentful if they didn't get a shift they wanted or if they think favoritism is occurring. ○ The Employee budget document is likely a sensitive work file because it could contain confidential and privileged information about the company's internal finances. ● *Is it safe to store personal files with work files?* ○ No, since a USB stick could easily get lost, stolen, or broken, it is not safe to store personal files and especially not safe to store work files. ○ Many companies have a strict policy against plugging in USB or other writable removable media into workplace computers. Some go so far as to keep computers in a locked cabinet to prevent theft and other devices from being plugged into them.
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *Could the information be used against other employees?* ○ *The new hire letter might reveal how much Jorge makes which could create animosity among various employees.* ○ *An attacker could rob Jorge's house while gone on vacation.* ○ *The shift schedules are a security risk because attackers could use it to determine when security guards are on break or not on duty if their shifts don't overlap.* ○ *Information in the Employee budget file could be used against Rhetorical Hospital.* ○ *The information on Jorge's resume could be used for*

	spearphishing attacks at his current or former employers by imitating someone of trust and trying to gain access to credentials or trick an employee into clicking on a suspicious link that causes malware to be downloaded. ○ This event could have been staged by a security professional to see who would pick up the suspicious flash drive and plug it in to a work or personal computer. ○ An attacker could have created fake files that actually install malware when clicked on. Moreover, they could have targeted Jorge personally by leaving the USB on the pavement where that employee typically parks. ● *Could the information be used against relatives?* ○ If the wedding list had PII, then spearphishing against them could happen, and a malicious actor would likely have their names, home addresses, and telephone numbers. They could also be robbed. ● *Could the information provide access to the business?* ○ Malware could provide access to the business by stealing, deleting, or locking files with ransomware. ○ The new hire letter, shift schedules, and employee budget could contain employee IDs and usernames that would be valuable to a hacker.
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* ○ If the USB were discovered by anyone not on the security team and plugged into any device that wasn't running virtualization and a sand-boxed environment, then it could have malware that could steal, delete, or lock data with ransomware or be used to gain access to critical systems and confidential information. ○ Other types of viruses, Trojans, and malware could be on this USB drive. ○ Even if no files were opened, sometimes malware can launch and install itself automatically once a flash drive is connected to a computer. ● *What sensitive information could a threat actor find on a device like this?* ○ As mentioned previously, several pieces of sensitive information could be found on a lost or stolen USB drive including compensation, usernames, employee IDs, shift schedules, staff hierarchies, company internal financial information possibly including account numbers, PII of wedding guests, and previous employers of Jorge that could be used for spearphishing, impersonation, or social engineering attacks. ● *How might that information be used against an individual or an organization?*

	○ Shift schedules being leaked could create a security risk for the company. A list of employee IDs and usernames would make it easier for a malicious actor to impersonate someone, spearphish, or brute force login. ○ Jorge's vacation plans could be used by a thief to rob their house while gone on vacation. ○ Employee compensation could be used by a competitor or create animosity with other employees of Rhetorical Hospital who feel that they are being unfairly compensated for their work. ○ Employee budget could contain confidential and privileged information about the company's internal financial situation that they might not want leaked to the media or competitors. This could also contain bank account numbers, which would make it more likely the company's bank accounts could be digitally robbed. ○ The PII of wedding guests could be used to rob them, send spearphishing emails, or use other social engineering tactics to pose a threat to them. ● *What are some technical, operational, or managerial controls that could mitigate these types of attacks?* ○ Many companies and organizations have strict policies about not plugging in USB devices or personal devices into workplace computers. ○ Some have parts of Windows disabled so that USB sticks cannot be accessed from within Windows explorer, and many have autoplay turned off so that Windows Explorer does not automatically open a the folder containing the contents of the USB drive. ○ Some companies even have employee workstations locked in a cabinet so that physical access to them is unavailable which prevents removable devices from being plugged into them and also prevents theft of devices.