

Parking lot USB exercise

Contents	<p>Write 2-3 sentences about the types of information found on this device.</p> <ul style="list-style-type: none">• Are there files that can contain PII? Yes the family photos in the USB are personally identifiable• Are there sensitive work files? Yes there are employee schedule files, employee budget files and a new hire letter• Is it safe to store personal files with work files? No it is not safe to store personal and work files together
Attacker mindset	<p>Write 2-3 sentences about how this information could be used against Jorge or the hospital.</p> <ul style="list-style-type: none">• Could the information be used against other employees? The information in the budget and schedule as well as personal resume details could be used against an employee.• Could the information be used against relatives? The information could be used to lean into a threat by showing family photos to the victim and demanding money or more. Vacation plans could be used to pose as a stalker to further implement fear• Could the information provide access to the business? If the budget and employee spreadsheets have email info in them then a email attach could be devised coupled with stealing an identity to establish trust
Risk analysis	<p>Write 3 or 4 sentences describing technical, operational, or managerial controls that could mitigate these types of attacks:</p> <ul style="list-style-type: none">• What types of malicious software could be hidden on these devices? Malware, Ransomware, Spyware, Trojans, Keyloggers, Rootkits, Viruses and Worms• What could have happened if the device were infected and discovered by another employee? spread of malware, data breach, ransomware attack, loss of trust• What sensitive information could a threat actor find on a device like this? PII, financial data, intellectual property, credentials

	<ul style="list-style-type: none">• <i>How might that information be used against an individual or an organization?</i> <i>Identity theft, financial fraud, corporate espionage, blackmail and extortion, credential stuffing.</i>
--	--