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?* ● *Are there sensitive work files?* ● *Is it safe to store personal files with work files?* *There are files that contain PII, such as the family photos and new hire letter. There are sensitive work files such as the new hire letter and employee shift schedule. It is not safe to store personal files with work files because it places both the organization and the individual at risk.*
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?* ● *Could the information be used against relatives?* ● *Could the information provide access to the business?* *The information could be used against other employees if for example an employee's schedule is compromised, enabling stalking, or an employee's pay is released from their hire letter. The information could also be used against relatives who may be included on the wedding invite list or in the family photos. The information may provide access to the business if an attacker is able to pose as a scheduled employee by presenting for their shift or intercepting the new hire letter to gain access to the building for orientation or training.*
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?* ● *What sensitive information could a threat actor find on a device like this?* ● *How might that information be used against an individual or an organization?* *One operational control that could be implemented is mandatory cybersecurity training that includes warning against inserting any discovered USB sticks into company devices. A managerial control that could mitigate attacks would be a company policy requiring any found USB sticks be handed over to the security team for testing and analysis. This would allow*

	trained professionals to test the USB in a controlled environment using virtualization software and determine the best course of action based on whether PII has been compromised or malicious software was attempted to be downloaded. A technical control that could mitigate these types of attacks would include requiring encryption of all company data stored on removable devices like USB sticks so that even if an attacker is able to obtain an employee's USB drive, they are less likely to be able to access the data stored on the drive. *Malicious software such as viruses or ransomware can be hidden on devices like USB sticks. If the device were infected and discovered by another employee, that employee could have unknowingly infected the network by plugging the device into a company computer. A threat actor could find sensitive information such as confidential marketing information for products that have not yet been launched or employee PII such as their addresses and names on devices like this USB stick. That information could be used against an individual and/or an organization because both could be held responsible for disclosure of PII, resulting in fines, loss of customer trust, and other negative outcomes.* *It's unsafe to plug an unfamiliar USB drive into your computer because of the wide range of attacks that can be hidden on them. Promoting employee awareness of USB baiting attacks is a managerial control that can reduce the risks of a negative event. Routinely scanning for viruses is an example of an operational control that can be implemented. And disabling Autoplay on all PCs is a technical precaution that can be taken.*