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?* *In this drive Jorge has stored a mixture of both personal and work files. Sensitive work files are present as both a new hire letter and employee budget file are present which likely has PII as well as the wedding list which likely includes names and emails. The general mixture of person and work files implies lacking security awareness on Jorge's part.*
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 offer letter likely has personal information regarding the new hire and potentially the person in control of hiring, maybe even Jorge himself as such a variety of attacks which involve impersonating different individuals can be executed. Being in possession of the wedding list would likely allow for a form of intimidation against Jorge's family as ominous emails could be sent likely coaxing further compromises of Jorges' families technology and information. It is also possible within the employee budget that information about HR is available enough to where the attacker could engage in social engineering to further escalate their privilege.*
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?* *The risks of these kinds of attacks is that if they are plugged into a computer with sensitive information or just generally a part of an organization's network it is possible for significant exploitation*

	to occur. Further due to the nature of a USB attack it may be possible that a machine is so completely compromised that tracking via logs of the initial breach becomes much more difficult especially if the USB is thrown away and the attacker stays for a long period of time as no logs would indicate something occured.