Parking lot USB exercise

Benjamin Taylor – Google Cybersecurity

Contents	Write **2-3 sentences** about the types of information found on this device. ● *This device contains important information, even some PII such as family photos.* ● *There are shift schedules, a new hire letter, and even a budget tracker. This means that all employment data is pretty much visible, from schedule to salary and company* ● *A resume is also present, detailing the person's past and work experience as well as skillset.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *This information is definitely capable of being used against Jorge and the hospital.* ● *There could be false threats made with Jorge's name, and with salary and shift being public record they could potentially mess with the hospital's operations.* ● *The attacker could pose as someone that Jorge knows or someone else in the hospital to create a malicious email and steal personal information from others as well.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *Promoting employee awareness about these sort of attacks and what to do when a suspicious USB drive is a managerial control that can reduce the risk of a negative incident.* ● *Setting up routine antivirus scans is another operational control that can be implemented.* ● *Disabling AutoPlay on company PCs can prevent the computers from automatically executing malicious code when USB drives are plugged in.*