Parking Lot USB Exercise

|  |  |
| --- | --- |
| Section | Response |
| Contents | The USB drive contains both personal and work-related files, including family and pet photos, a new hire letter, and an employee shift schedule. This mix of information could expose personally identifiable information (PII) and sensitive organizational data, making the device a potential target for attackers seeking to exploit weak points in the hospital's security. |
| Attacker Mindset | An attacker could use the contents of this USB drive to gather intelligence about Jorge Bailey and Rhetorical Hospital. For example, the shift schedule could reveal employee routines, while the new hire letter might expose internal policies. The personal content might also be used for social engineering attacks, such as phishing or identity theft. |
| Risk Analysis | USB baiting attacks pose significant threats, including the potential delivery of malware such as keyloggers, ransomware, or remote access trojans (RATs). If another employee had picked up and opened this USB drive on a non-isolated system, the hospital’s network could have been compromised. To mitigate these risks, technical controls like disabling USB ports and using endpoint detection software should be implemented. Operational controls include regular cybersecurity training and awareness campaigns. Managerial controls could involve policies for reporting and handling found devices, as well as maintaining strict data handling procedures. |