Parking lot USB exercise

Maria Audu

Contents	*. The USB drive contains a mixture of personal and work-related files, such as emails, employee contact information, project documents, and possibly login credentials. It may also hold sensitive hospital data like internal policies or patient-related information. This combination of data makes the USB potentially valuable to attackers.*
Attacker mindset	*An attacker could use the files to target Jorge or other hospital staff through phishing, social engineering, or impersonation. Internal documents and personal data could help plan more advanced attacks. The hospital logo increases trust, making it more likely an employee would plug the drive into a workstation.*
Risk analysis	*USB baiting attacks could deliver malware such as ransomware, spyware, or remote access tools, compromising hospital systems and sensitive data. Threat actors could steal, modify, or misuse information to target staff or the organization. Controls like disabling unused USB ports, endpoint protection, and sandbox testing reduce exposure. Employee training and strict USB policies further help mitigate risks and prevent accidental infections.*