## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | The USB device contains sensitive information, including Jorge’s personal documents (e.g., financial records or private communications) that could harm his reputation if exposed. Additionally, work files store **Personally Identifiable Information (PII)** of others (e.g., patient or employee data) and confidential details about the hospital’s internal operations, such as schedules or protocols. |
| **Attacker mindset** | An attacker could exploit this data to launch **targeted phishing campaigns**—for example, impersonating a coworker using timesheet details to trick Jorge into sharing credentials. The hospital’s operational information might enable **ransomware attacks** (e.g., disrupting critical workflows) or selling stolen PII on the dark market, harming both Jorge’s credibility and the hospital’s compliance with privacy laws. |
| **Risk analysis** | To mitigate USB-based risks, **technical controls** like encrypting devices, deploying EDR tools, and disabling AutoPlay can block malware execution. **Operational controls** include enforcing USB usage policies, routine antivirus scans, and automated log monitoring to detect suspicious activity. **Managerial controls** such as mandatory employee training, incident response plans, and disciplinary measures for policy violations foster a security-aware culture. Together, these layered defenses reduce vulnerabilities by combining technology, processes, and governance to protect against both physical and digital threats. |