## **Parking lot USB exercise**

| **Contents** | * The USB drive contains a mix of personal and sensitive work-related information, including shift schedules, an employee budget, a new hire letter, and Jorge Bailey’s resume. Some files contain personally identifiable information (PII), such as names, employment details, and potentially addresses. Storing personal files like vacation plans and wedding lists alongside hospital documents creates a security risk and violates best practices for separating personal and professional data. |
| --- | --- |
| **Attacker mindset** | * *An attacker could use the resume or HR documents to launch targeted phishing attacks on Jorge or other employees. The employee shift schedule and budget files might reveal internal operations that could be exploited to gain further access to hospital systems. The mix of personal and professional content may also help an attacker build social engineering profiles to impersonate Jorge or manipulate his contacts.* |
| **Risk analysis** | * Even if this USB drive is not infected, it still poses a significant threat because it could have been used in a USB baiting attack. If it had contained malware, another employee might have unknowingly executed malicious code, enabling data exfiltration or unauthorized access. Technical controls like disabling USB ports and enforcing endpoint protection can help. Managerial controls include employee education about USB risks and implementing policies to report and isolate found devices before inspection. |