**Contents**

The USB drive contains both personal and work-related files, such as family and pet photos, a new hire letter, and an employee shift schedule. These files likely include personally identifiable information (PII) like names and addresses. Storing personal and work files together on the same device is risky, as it increases the potential for sensitive data to be exposed.

**Attacker Mindset**

An attacker could use the information on the USB drive to target Jorge or the hospital. The PII from the personal photos and documents could be used for identity theft or phishing attacks. Additionally, work-related files, such as the new hire letter and shift schedule, could provide insights into the hospital's operations, making it easier for the attacker to plan further attacks or gain unauthorized access to the hospital’s systems.

**Risk Analysis**

USB baiting attacks can hide various types of malicious software, such as keyloggers, ransomware, or backdoors that allow attackers to access a network remotely. If this USB drive had been infected and discovered by another employee, it could have compromised the hospital's network, leading to data breaches or system disruptions. To mitigate these risks, technical controls like disabling USB ports, operational controls like employee training on the dangers of unknown USB devices, and managerial controls like enforcing strict policies on data storage and device use should be implemented.

Principio del formulario

Final del formulario