Identifying Attack Vectors

Scenario

I am part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. You bring the USB drive back to your office where the team has virtualization software installed on a workstation. This simulation isn't connected to other files or networks, so the USB drive can't affect other systems if it happens to be infected with malicious software.

Analysis

Contents	Jorge's USB drive contains both personal and professional data. Specifically, it holds family and pet photos, which are private in nature. Additionally, there are official documents like a new hire letter, an employee shift schedule, and an employee budget tracker which could contain sensitive work-related information. It's not recommended to mix personal files with work files due to potential security risks.
Attacker Mindset	If an attacker accessed the device, they could exploit Jorge's personal information for social engineering tactics or blackmail. The work files could provide insights into the hospital's operations, and potentially be used for corporate espionage or manipulation. Furthermore, if the event was staged, using the USB could have provided unauthorized access into the hospital's IT infrastructure.
Risk Analysis	To mitigate risks associated with USB baiting attacks, Rhetorical Hospital could: • Implement a policy against using personal USB drives on work systems. • Educate employees about the dangers of plugging in unknown USB drives and the risks of mixing work and personal data. • Use endpoint protection software to scan and block potentially malicious software. • Employ network monitoring to detect unusual activities or unauthorized access attempts.