# Parking lot USB exercise

## Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are 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. There’s no one else around who might have dropped it, so you decide to pick it up out of curiosity.

You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it’s one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same 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.

| | |
|---|---|
| **Contents** | The USB stick contains a mix of personal and sensitive information. Among the documents are files containing personal information of individuals, including Jorge's own data that he would prefer to keep private. Additionally, there are work files that provide insights into the hospital's operations and procedures. |
| **Attacker mindset** | The information found on the USB stick, such as the timesheets containing details about Jorge's colleagues, poses significant risks for both Jorge and the hospital. Malicious actors could exploit this information to deceive Jorge through various means, including phishing attacks. By crafting convincing emails or impersonating trusted individuals, attackers could manipulate Jorge into disclosing sensitive data, compromising the hospital's security, or gaining unauthorized access to its systems. |

| | |
|---|---|
| **Risk analysis** | Promoting comprehensive employee awareness and providing regular training on recognizing and handling suspicious USB drives is a crucial managerial control that can effectively mitigate the risk of such incidents. Implementing a robust operational control involves conducting routine antivirus scans on all systems to detect and prevent any malware introduced through USB drives. Additionally, employing technical controls, such as disabling AutoPlay functionality on company PCs, adds an extra layer of defense by preventing automatic execution of malicious code upon connecting a USB drive, thereby minimizing the risk of infection and compromise. It is important to note that a combination of these controls working in tandem can significantly enhance the overall security posture of the organization. |