Parking lot USB

Scenario

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	Yes, there are files on Jorge's USB drive that can potentially contain Personally Identifiable Information (PII). This includes personal photos and possibly information in the new hire letter and employee shift schedule. Mixing personal files with sensitive work-related data on the same drive is generally not safe, as it can pose security and privacy risks. It's advisable to keep personal and work files separate to minimize these risks and protect sensitive information.
Attacker mindset	Yes, the information on Jorge's USB drive could potentially be used against other employees if it falls into the wrong hands. For instance, sensitive work-related data like the employee shift schedule could be exploited to gain insights into the company's operations or potentially disrupt them. Likewise, if there are personal files containing information about Jorge's relatives, this information could also be misused for malicious purposes. Furthermore, if any of the work-related files contain access credentials or sensitive business information, they could provide unauthorized access to the business, leading to security breaches. Hence, it's crucial to handle and store such data securely to prevent these risks.

Risk analysis	Several types of malicious software, including malware, spyware, or ransomware, could be hidden on these devices. If the device were infected and discovered by another employee, it could lead to various negative consequences. For instance, malware could compromise the security of the device and potentially spread across the network, impacting the organization's overall cybersecurity. A threat actor could find sensitive information such as personally identifiable information (PII), confidential work documents, employee schedules, and personal data on this device. This information could be used against an individual through identity theft, blackmail, or phishing attempts. Additionally, if work-related documents contain proprietary business information or trade secrets, they could be used maliciously to gain a competitive advantage or sold on the black market, posing a significant risk to the organization's reputation and operations. Therefore, it's essential to maintain strict security protocols for such devices to prevent these potential threats.