Parking Lot USB drive

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.

Jorge's drive contains a mix of personal and work-related files. For example, it contains folders that appear to store family and pet photos. There is also a new hire letter and an employee shift schedule. The flash drive appears to contain a mixture of personal and work-related files. Consider how an attacker might use this information if they obtained it. Also, consider whether this whole event was staged.

Solution

Points	**Description**
Contents	Not all documents contain personal information. However, Jorge would not want them to be made public anyway. Some of the work files include personal information and its hospital's operations.
Attacker mindset	The information that the attackers would obtain could benefit them to trick Jorge. Now, they can send malicious email to manipulate Jorge to obtain more personal information (Payment cards and more).
Risk analysis	Educating all employees about these types of attacks can raise awareness and prevent the incident from happening again. This is a managerial control. Second, setting up a protection system, such as installing antivirus and scanning the device on a regular basis is an operational control. Third, to prevent malicious code from being executed when a USB drive is plugged in, we can disable "the autoplay" feature or make sure the file has to be sent through an email address that has antivirus in it.