Parking lot USB exercise

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	*Upon checking the contents of the drive, it contains a mix of personal and work-related stuff. This includes the following:* ● *Employee Budget* ● *Shift schedule of Rhetorical Hospital* ● *Wedding lists* *These are sensitive data is not safe to be stored in a USB.*
Attacker mindset	*With these sensitive data, this information could be used against other employees as it contains the schedule.* *This can be used against other members as found on the wedding lists. The attacker might get their information and can cause harm.* *This could also harm the business as it contains budget details as well. The attacker also uses this as a medium to infiltrate the organization by deploying malicious software and damage the reputation of the organization.*

Risk analysis	The type of information stored in this device are sensitive information. This contains personal and work information. This information can be used against the owner or the organization. The attacker can inflict damage to the owner or to the organization with malware when plugged into a computer directly. The malware then downloads a malicious code into the device that could fetch information and steal them. To mitigate this risk, it is recommended to use passwords and encryption on the USB to protect the data. It is also advisable to disable autoruns. This can prevent malicious code on an infected USB drive from opening automatically. Lastly, keep personal and business USB drives separate.