Parking lot USB exercise

Contents	This USB drive has various forms of PII as well as potentially sensitive work files such as shift changes stored inside. From this USB, we can tell the owner's name is Jorge. Jorge works at a hospital and is set to marry Wendy in June. We can also see information about other employees at the hospital, as well as the hospital's budget.
Attacker mindset	These file leaks could potentially be used against Jorge if they were to get into the wrong hands. As an example, a malicious actor would have various forms of work and personal information that could be used in order to trick Jorge into opening a seemingly safe email that puts a virus on his computer.
Risk analysis	There are many ways to help prevent and/or mitigate these types of attacks. Some of these examples include setting up regular antivirus scans to make sure all PC's are safe, and setting precautions by disabling the auto open feature when plugging in a USB. This may prevent the malicious code from executing.