## **Parking lot USB exercise**

| **Contents** | *Within this USB drive, there is both work-related files and personal information. This contains information like: New hire letter, shift schedules, personal wedding list, the HR representatives resume, employee budget, family photos and more. There is sensitive personal information and PII within these documents. Storing personal information with work-related files is not an optimal security practice.* |
| --- | --- |
| **Attacker mindset** | *There are many areas an adversary could exploit with a malicious USB. If they were targeting the company, this could allow them access to employees in the organization, the internal database, or even apply a backdoor to attain persistence within the network servers. They can also use this to target Jorge’s family, or his own home by getting access to personal information. There are a multitude of different options an adversary could use to exfiltrate information with USB baiting.* |
| **Risk analysis** | *This has the potential to be a much more dangerous incident if the USB had fallen into the wrong hands. The USB could have been written with malicious code, which could have had the ability to take control of the computer, its programs, or even gain persistence over the network. Critical data could have been exfiltrated, or even a ransomware attack where a payment would be necessary to regain control of internal servers. Personal information could be leaked, therefore harming the reputation of the organization and impacting business continuity.* |