## **Parking lot USB exercise**

| **Contents** | There are multiple files in there which can pose a significant threat to Jorge both professionally and personally as there are details about his wedding slides and family photos and resume which contains PII and also employee budget, shift schedules which could cause huge threats to the organization if it falls into the wrong hands. And it is not safe to store both personal and work files in the same place as there are multiple policies against that. |
| --- | --- |
| **Attacker mindset** | The attacker can use the information found here to do a phishing scam on their family members and also use social engineering attacks posing as a different doctor who works on a different schedule to gain access to restricted areas. Can also sell this data to a competitor for profit. |
| **Risk analysis** | In terms of technical we can make the USB drive password protective and make sure it has a password to access the files in the USB stick. And also promoting awareness about rogue USB sticks to employees would be beneficial and also developing policies like not mixing work and personal files would be better for the future of the organization and also make sure AutoPlay is disabled to block any malicious code from entering the system. |