## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | *The USB flash drive contains PII not just from the owner who works in the hospital nor other workers and owner’s family too such shift schedules, signed letters. It is not secure to mix work and personal files in the same asset.* |
| **Attacker mindset** | *The data contained here can be used to track hospital workers and the owner, and finally the information about business operations can be an attack vector also can originate physical attacks and digital.* |
| **Risk analysis** | *Exist the risk that malicious actor can inject worms, autokey loggers and ransomware if another worker discovered the USB before Security team, this works automatic will be a vector attack. If a malicious actor had obtained the USB before he could have obtained PII and orchestrated physical attacks against workers or digital attacks against hospital systems, in this example he could do analysis of who has enough authority to start his attack by defining his target.* |