## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | *Thje drive contained files that were personal in nature including his resume, vacation ideas, etc. and work related files.The files expose some PII information about Jorge and could be as part of identity thief scenario. The work related information on the USB might be a starting place for recon on the company that Jorge works for. Information found in the files maybe added to a digital footprint scan of the companies digital presents to determine attack vectors.* |
| **Attacker mindset** | *The data could be used against the individual and hospital.*  *Dates and times of when Jorge will be out of town for vacations\weddings for additional information searches at his residents. Address supplied in his resume.*  *Shift schedules might show times when attention is low for a physical or social engineering attack on the hospital.* |
| **Risk analysis** | *The USB could be have been a trojan horse attach to get malware or a virus into to the network to create an avenue for future attacks or cause damage to company assests. The USB drive could used to develop as part of a recon of the companies digital footprint and assets for future attacks or actiivities. The mixure of personal and company information could be used to used in combination to embarrass the individual and\or company for the security posture related to a hospital that maintains health data on individuals.* |