## **Parking Lot USB Exercise**

| **Contents** | There are a multitude of files both personal and work related on the USB drive belonging to Jorge Bailey   * There is a substantial amount of PII in the contents both pertaining to the owner (Jorge Bailey) as well as work related such as information in the found resume and employee shifts documents * It is not a good idea to store both personal and work related items on the same USB drive. Separation of personal and work helps to ensure sensitive materials don’t end up where they shouldn’t be. |
| --- | --- |
| **Attacker mindset** | The USB drive would give an attacker several methods to attack.   * Jorge’s personal family photos and wedding invitation could be used for blackmail to gain more sensitive information. * Other hospital employee shifts are exposed giving an attacker PII information like employee names and shift times * Sensitive hospital information is exposed like the budget proposal or the new hire resume (could expose the hospital to litigation if discovered PII was exposed by the negligence of staff. |
| **Risk analysis** | While the USB drive proved to not have malicious software it did contain documents consisting of various forms of PII that could be damaging if exposed.   * Personal and work related information should not be stored on the same USB stick. Separating the two reduces the likelihood of information falling into the wrong hands. * Had another employee happened to find and use the USB there is a high likelihood of malicious software compromising the used device and spreading to the network and other devices.   + In this case though there was no malicious software there was still documents with sensitive information that should not be exposed to just any employee. * Work related files on a separate USB should also be encrypted. This reduces the chances of sensitive information being leaked in the result of the USB being stolen or misplaced. |