## **Parking lot USB exercise**

| **Contents** | In this USB drive or Jorge’s USB contain PII, personal files and sensitive work files. The file that can be exploited for PII is the new hire file, beside it containing the sensitive work files it also contains other people's email and his email address. As for the personal files can be obtained from the family and pet photos, as for the sensitive work files can be obtained from shift schedules, new hire letter employee budget files. Storing personal files with work files on the same drive is not a good way to do because it can create a risk of exposing sensitive work-related information for personal use |
| --- | --- |
| **Attacker mindset** | The attacker could potentially use the information from the USB drive to get intel about the other employee from the hospital or Jorge to impersonate them in order to get access to the business system. As the attack could be used against relatives too for example they might use the personal photos to craft convincing social engineering attacks or use the work-related files for spear-phishing. |
| **Risk analysis** | Promoting awareness about the types of attack such as a suspicious risk that is associated with a USB drive. While a USB drive doesn’t appear to contain malicious code in the operational control. Because while it does not seem to be malicious, it still poses a security risk. An attacker could hide various types of malicious software on such devices that potentially lead to an infection to the hospital network or server system which can lead to a breach to the sensitive information that can be used for impersonation, social engineering, or targeted attacks against Jorge or the hospital. To prevent this the next step can be done by doing the technical control such as applying and maintaining the security software and keeping all software uptodate such as firewall, antivirus, spyware or disable Autorun for CD/DVD/USB drives to prevent them to open automatically when they are inserted into a drive. The managerial controls can be done by making a strict USB drive usage policy. Additionally keeping personal data and business data separate is a good way to reduce risk associated with data breach from USB drive or USB baiting. |