## **Parking lot USB exercise**

| **Contents** | The usb contains personal PII and employee PII and potentially SPII.  It several things that aren’t work related such as:   * Photos * Wedding list * Vacation ideas * Personal Resume   Several work related pieces of information:   * New hire letter * Employee budget * Employee schedule |
| --- | --- |
| **Attacker mindset** | An attacker could use his personal information, his family photos and vacation plans to scare him into providing inside information, remote access, logins, etc by threatening his family and blackmailing.  You can also use the new hire letter to better understand what a new employee might go through to better help get an insider hired and into the company. The budget information besides potentially containing SPII can be used to maybe out bid another company.  The employee schedule can be used to stalk and social engineer other employees or maybe locate when a particularly new employee will be working so they can be more easily exploited.  You can place malware on it and if itwas found and plugged in then it could have infected the hospital's computer systems in any number of ways from ransomware to keyloggers.  This usb could have contained SPII that can be sold and used for identity theft. |
| **Risk analysis** | Disabling all USB ports across the hospital and whitelisting company issued peripherals such as dell keyboards and mice. If flash drive usage is required then the hospital can provide company issued drives which have been whitelisted by hardware ID.  Enable logging for USB ports so if an non whitelisted device is connected it will create a log and send an alert, also logging all reads and writes to log what is being taken and put into the system by the company USB’s.  New technology usage policy that prohibits using the company usb for personal files and prohibits using any none company equipment. |