## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | Write **2-3 sentences** about the types of information found on this device.   * *Are there files that can contain PII?* * *Are there sensitive work files?* * *Is it safe to store personal files with work files?*   *Upon investigation of the USB drive found in the parking lot of Rhetorical Hospital, it was revealed to contain a mix of administrative documents, employee personal identifiable information (PII), and sensitive health records of patients. Among these files, there are Excel spreadsheets with employee contact details and PDF files of patient records, which clearly contain PII. Additionally, there are mixed personal files, including photographs and documents, likely belonging to an employee. Storing personal files with work files on a USB drive, especially one not encrypted, poses a significant risk as it increases the chances of sensitive information being mishandled or accessed by unauthorized individuals.* |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.   * *Could the information be used against other employees?* * *Could the information be used against relatives?* * *Could the information provide access to the business?*   *The information found on this USB drive could be highly valuable from an attacker's perspective. Not only could the PII be exploited for identity theft against Jorge or other hospital employees, but access to patient health records could also lead to targeted phishing attacks, blackmail, or even medical fraud. The presence of sensitive work files alongside personal files might indicate lax security practices, making the hospital and its employees prime targets for further exploitation. Additionally, if this USB drive fell into the hands of a competitor or a criminal organization, it could provide them with unauthorized access to the hospital’s network, potentially leading to a larger breach* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:   * *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* * *What sensitive information could a threat actor find on a device like this?* * *How might that information be used against an individual or an organization?*   *To mitigate the risk of USB baiting and other related attacks, several technical, operational, and managerial controls are necessary. Technically, the hospital should employ endpoint security solutions that restrict or monitor USB access on organizational devices, alongside the use of encryption for any USB drive containing sensitive information. Malicious software that could be hidden on such devices includes ransomware, keyloggers, or backdoors that could compromise the hospital’s network. If this device were infected and discovered by an uninformed employee, it could lead to a data breach or a network-wide infection, compromising patient confidentiality and the hospital's operational integrity. To prevent misuse of information found on such devices, comprehensive training on data protection and cybersecurity best practices for all employees is crucial. This should be coupled with a clear policy on the use of external storage devices and regular security audits to ensure compliance and identify potential security gaps.* |