**Weekly Report <WeekNumber: 1>**

**Capstone Project**

# **Participant name: RAJAN KUMAR SAHU**

# **Name / Title of the Project: Leadership capstone**

*Please share the details of the tasks completed. We have given 4 tasks as a template, if you have completed more tasks, please remove the additiional task headings.*

*In case you are attempting both versions of the capstone, please indicate your progress for both the capstone projects.*

**Tasks completed:**

1. Task 1: Risk identification:

* Hardware Assets: Laptops: 7 laptops with missing critical files and low disk space.

USB drives: The personal USB drive used to copy the pirated movie.

* Network Assets:
* Internet access: Employees have unrestricted internet access, which could potentially introduce security risks.
* Data Assets:
* Critical files: Files that went missing from the 7 laptops, potentially indicating data loss or compromise.
* Email Assets:
* Email system: The email from Mike Parry requesting the transfer of funds was fraudulent, suggesting a possible vulnerability or compromise in the email system.
* Financial Assets:
* Transferred funds: $10,000 transferred to an overseas bank based on the fraudulent email.
* Human Assets:

Employees: The actions of an employee downloading pirated content and copying it to a personal USB drive contributed to the security incident.

Information Security Assets:

Security controls: It's evident that the organization lacks sufficient security controls, such as restrictions on internet access and email authentication measures.

1. **Task 2: Risk Assessment:**

**Unauthorized downloading and piracy:**

Risk: An employee downloaded pirated content, leading to a lawsuit from Sony pictures and potential legal consequences for Enablers INC.

Risk Severity: High

Reference: Legal ramifications of piracy and copyright infringement.

Data breach and loss of critical files:

Risk: Seven laptops reported missing critical files, possibly due to malware or unauthorized access.

Risk Severity: High

Reference: Best practices for data security and prevention of data breaches.

**Social engineering and financial fraud:**

Risk: An employee fell victim to an email scam, resulting in the transfer of funds to an unauthorized overseas account.

Risk Severity: High

Reference: Awareness of common email scams and best practices for preventing social engineering attacks.

**IT system vulnerabilities:**

Risk: The conference call indicates a lack of clarity on next steps, suggesting potential IT system vulnerabilities or weaknesses.

Risk Severity: Medium

Reference: IT security frameworks and best practices for incident response and system security.