**Weekly Report <WeekNumber: 2>**

**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 3: Identify applicable controls for risk treatment:

* Regular Security Audits: Conduct periodic security audits and assessments to identify vulnerabilities, assess the effectiveness of existing controls, and implement necessary improvements. This can help proactively identify and address potential security gaps.
* Incident Response Plan: Develop an incident response plan that outlines the steps to be taken in the event of security incidents, such as data breaches, malware infections, or fraudulent activities. Define roles, responsibilities, and communication channels to ensure a coordinated and effective response.
* Data Backup and Recovery: Establish a robust data backup and recovery strategy to ensure that critical files are regularly backed up and can be restored in case of data loss. This can help mitigate the impact of incidents like missing critical files on laptops.
* Endpoint Protection and Data Loss Prevention: Deploy endpoint protection solutions that include features such as antivirus/anti-malware, firewall, and data loss prevention (DLP) mechanisms. These measures can help identify and block malicious activities, detect unauthorized file transfers, and safeguard critical company data.

1. Task 4: Evaluating the controls:

* Acceptable Use Policy (AUP): Develop and communicate a clear AUP that defines acceptable internet usage, including restrictions on downloading copyrighted content, using unauthorized software, and connecting personal devices to company systems.
* Endpoint Security Measures: Implement robust endpoint security solutions with features such antivirus/anti-malware software, firewall, and regular system updates. This will help protect against malware infections, data breaches, and unauthorized access.
* Email Security Measures: Strengthen email security by implementing email filtering, anti-spam mechanisms, and user awareness training to mitigate the risk of email-related scams, phishing attempts, and fraudulent activities.
* Security Awareness and Training: Conduct regular security awareness programs and training sessions to educate employees about cybersecurity best practices, including recognizing phishing attempts and the importance of adhering to company policies.

[***david@ultraenablers.com***](mailto:david@ultraenablers.com)write an email **:**

Dear David,

I hope this email finds you well. I am writing to provide an update on the recent security incidents we have faced at Enablers Inc. and to request your approval and budget for implementing necessary security controls based on the risk assessment conducted.

As you are aware, we have experienced several incidents that have exposed our organization to significant risks. Firstly, we received a lawsuit from Sony Pictures due to an employee downloading uTorrent software and using it to download a pirated version of the movie "Pirates of the Caribbean." Additionally, we encountered issues where critical files went missing on 7 company laptops, resulting in low memory and disk space. Moreover, an employee fell victim to an email scam, transferring $10,000 to an overseas bank after receiving a fraudulent email that appeared to be from Mike Parry.

In light of these incidents, we have conducted a comprehensive risk assessment to identify the controls required to mitigate these risks and strengthen our security posture. After careful evaluation, we have identified the following controls that need to be implemented:

1. Task 5: Evaluating the vendors:
2. Endpoint Security Solution:

* Vendor: Symantec (now NortonLifeLock)
* Product: Norton Endpoint Protection

Features:

Antivirus/anti-malware protection to detect and prevent malware infections.

Firewall protection to block unauthorized access and control network traffic.

Advanced threat detection and behavior monitoring to identify and stop emerging threats.

Web filtering and content control to restrict access to malicious websites and enforce acceptable internet usage policies.

Centralized management console for easy deployment, monitoring, and reporting.

1. Data Backup and Storage Solution:

Vendor: Veeam Software

Product: Veeam Backup & Replication

Features:

Automated and reliable backup of critical files and data with flexible scheduling options.

Incremental and differential backup to reduce storage requirements and backup time.

Data deduplication and compression to optimize storage space.

Encryption of backup data to ensure confidentiality and integrity.

Offsite backup and replication for disaster recovery purposes.

Granular file-level and application-level recovery options.

1. Email Security Solution:

Vendor: Proofpoint

Product: Proofpoint Email Protection

Features:

Advanced email filtering and anti-spam mechanisms to block malicious emails and phishing attempts.

URL protection and click-time protection to identify and prevent users from accessing malicious websites.

Email encryption and data loss prevention (DLP) to secure sensitive information and prevent data leaks.

Threat intelligence and machine learning algorithms to detect and mitigate evolving email threats.

User awareness training modules to educate employees about email security best practices and phishing awareness.

Considering the specific requirements and risks faced by Enablers Inc., I would recommend choosing the email security solution provided by Proofpoint. This solution offers a comprehensive set of features to protect against email-related risks, including phishing attempts, malware-laden attachments, and malicious URLs. Its robust threat intelligence and machine learning capabilities ensure proactive detection and mitigation of evolving email threats. The user awareness training modules further strengthen the organization's overall security posture.

It is important to note that vendor selection should be based on a thorough evaluation of the organization's specific needs, budget, and compatibility with existing systems and infrastructure. Additionally, engaging in a vendor evaluation process, including product demonstrations, requesting references, and assessing pricing and support options, will help make an informed decision.