Capstone Final Report- PGPCS Jun 2023

<Rajan Kumar Sahu>

*Capstone Final report showcases the final learnings and outcomes of the project. The write up must adhere to the guidelines and should include the following.*

# Objectives completed:

* Founding the organization: Mike Parry and Pam Trotter founded Enablers INC in 2020 at the beginning of the pandemic.
* Securing funding: In 2021, Enablers INC received a funding of 10 Million USD, which boosted their ambitions and allowed them to expand their operations.
* Hiring a team: Enablers INC hired a team of 20 individuals to work for the organization.
* Setting up an office: The organization rented an office space for their operations.
* Providing internet access: The founders ensured that the employees have unrestricted access to the internet, emphasizing the importance of freedom in accessing online resources.

some challenges and issues:

* Lawsuit from Sony Pictures: Enablers INC received a lawsuit from Sony Pictures due to one of their employees downloading a pirated version of the movie "Pirates of the Caribbean" using uTorrent software and subsequently copying it onto a personal USB drive.
* Missing files and low disk space: Several company laptops reported missing critical files and low disk space, indicating a potential data loss or storage issue.
* Email scam: An employee received an email from someone posing as Mike Parry, requesting a money transfer to an overseas bank. The transfer was made, but it was later discovered that the email was not genuine.
* IT troubleshooting: Aaron, the head of IT, initiated a conference call to address the issues, but after three hours of troubleshooting, the next steps to resolve the problems remained unclear.

# Risk Identification and Assessment:

*Use the risk assessment sheet (workbook) and the risks identified from the case study. Prefer using a tabular format for better visibility and presentation.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset** | **Category** | **Threat** | **Vulnerability** | **Asset Value**  **(1 to 4)** | **Threat value (1 to 2)** | **Vulnerability Value (1 to 2)** | **Overall Risk (1 to 16)** |
| Laptops | Hardware | Malware | Unrestricted Internet Access | $10,000 Financial Assets | Malware | Unrestricted Internet Access | Assign a numerical value to each threat, vulnerability, and asset based on its perceived severity and impact. |
| Internet access | Network | Data Breach | Lack of Security Policies | Data Assets | Data Breach | Lack of Security Policies and User Training | Assess the likelihood of each threat occurring and the likelihood of each vulnerability being exploited. |
| USB drives | Data | Insider Threat | Insufficient User Training | Hardware Assets | Insider Threat |  | Multiply the severity/impact value by the likelihood value for each threat and vulnerability. |
| Email system | Email | Social Engineering | Weak Endpoint Security | Email Assets | Social Engineering |  | Sum up the calculated values for all threats and vulnerabilities. |
| Financial assets | Transferred funds | Lack of Security Controls | Lack of Data Backup |  |  |  |  |
| Employees | pirated content | Reputation Damage | Inadequate Email Authentication |  |  |  |  |

# Risk to control mapping:

*Map the risks to required controls, evaluate the controls and identify the products/services required. Use a tabular format where you mention the risks, the respective controls and the products and services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Control** | **Features Required** | **Additional comments** |
| Risk of Malware Infections | The unrestricted internet access and the employee's use of uTorrent software to download pirated content introduces the risk of malware | Secure Internet Access | Security Culture: Building a strong security culture within the organization is crucial. This involves fostering a sense of responsibility and awareness among employees regarding cybersecurity best practices. |
| Risk of Data Breach | missing critical files on the laptops indicate a potential data breach or unauthorized access to sensitive information, | Endpoint Protection | Incident Response Team: Establish an incident response team composed of representatives from IT, security, legal, and management departments |
| Financial Risk | The organization experienced a financial loss of $10,000 due to the fraudulent email and unauthorized funds transfer. | Data Loss Prevention | Third-Party Risk Management: Evaluate and manage the risks associated with third-party vendors, contractors, or partners who may have access to the organization's systems or data |
| Reputation Risk | he lawsuit from Sony Pictures due to the employee's downloading of copyrighted content can damage the organization's reputation. | Regular Security Audits and Updates | Regular Security Assessments: Conduct periodic security assessments, including vulnerability scanning, penetration testing |

* *Unauthorized downloading and sharing of copyrighted content:*

*Implement an Acceptable Use Policy (AUP) that clearly states the restrictions on downloading and sharing copyrighted material.*

*Deploy web filtering or firewall solutions to block access to websites or software known for facilitating illegal downloads.*

*Educate employees about copyright laws and the consequences of illegal downloading.*

* *Data loss and low disk space:*

*Regularly back up critical files and data to a secure and reliable storage system.*

*Implement disk space monitoring tools to proactively identify and address low disk space issues.*

*Enforce policies on data storage and retention, including guidelines on deleting unnecessary files and proper use of cloud storage.*

* *Email scams and phishing attacks:*

*Implement strong email security measures, such as spam filters and email authentication protocols (e.g., SPF, DKIM, DMARC).*

*Conduct employee training on email security, phishing awareness, and how to identify suspicious emails.*

*Implement multi-factor authentication (MFA) for email accounts to prevent unauthorized access.*

* *IT security incident response:*

*Develop an incident response plan that outlines the steps to be taken in the event of a security incident.*

*Regularly test and update the incident response plan to ensure its effectiveness.*

*Conduct thorough investigations and forensic analysis to determine the source and extent of security incidents.*

*Enhance security controls, such as network monitoring, intrusion detection systems, and endpoint protection, to detect and prevent security breaches.*

* *Access controls and user permissions:*

*Implement strong access controls and user permissions to limit employee access to sensitive systems and data.*

*Use role-based access controls (RBAC) to ensure employees have access only to the resources necessary for their roles.*

*Regularly review and update user access privileges to reflect changes in job responsibilities or departures of employees.*

* *Employee training and awareness:*

*Provide comprehensive training programs to educate employees about security best practices, such as safe internet usage, recognizing social engineering techniques, and adhering to company policies.*

*Regularly communicate security updates, reminders, and policy changes to keep employees informed and vigilant.*

*It's important to note that the specific control measures may vary depending on the organization's size, industry, and regulatory requirements. Implementing a comprehensive information security program and regularly assessing and updating the controls can help mitigate risks and enhance the organization's overall security posture.*

# Control implementation plan:

*For each control, prepare an implementation plan with the following elements:*

* ***Type of control:***

1. Administrative Controls: These controls focus on establishing policies, procedures, and guidelines to manage and mitigate risks. Examples include:

# Implementing an Acceptable Use Policy (AUP) to govern employee behavior regarding downloading copyrighted content.

# Developing an incident response plan and conducting employee training on security best practices.

# Technical Controls: These controls are implemented through technology and aim to protect systems, networks, and data. Examples include:

# Deploying web filtering or firewall solutions to block access to websites known for illegal downloads.

# Implementing disk space monitoring tools to identify and address low disk space issues.

# Physical Controls: These controls are physical measures to safeguard physical assets and restrict unauthorized access. While not explicitly mentioned in the scenario, they could include measures such as:

# Implementing access controls to the office premises to prevent unauthorized individuals from entering.

# Protecting server rooms and critical infrastructure with physical security measures like locks and surveillance systems.

# Awareness and Training Controls: These controls focus on educating employees about security best practices and raising awareness about potential risks. Examples include:

# Conducting employee training on email security, phishing awareness, and recognizing social engineering techniques.

# Regularly communicating security updates, reminders, and policy changes to employees. ng plan:

* **Control ownership:** Control ownership refers to the responsibility and accountability for the implementation, management, and effectiveness of specific controls within an organization. In the scenario provided, control ownership can be attributed to different individuals or teams based on their roles and responsibilities.

**Acceptable Use Policy (AUP) and policy enforcement:**

Ownership: Human Resources (HR) or Legal Department

Responsibilities: Developing and maintaining the AUP, ensuring compliance, and enforcing policy violations.

**Web filtering and firewall solutions:**

Ownership: IT Department or Network Security Team

Responsibilities: Selecting, implementing, and managing web filtering and firewall technologies to block access to restricted websites and monitor internet traffic.

Disk space monitoring tools:

Ownership: IT Department or System Administrators

Responsibilities: Deploying and managing disk space monitoring tools to track storage usage, identify low disk space issues, and take necessary actions to mitigate the problem.

**Coverage of the control:**Coverage of controls refers to the extent to which the controls implemented by an organization address the identified risks and protect against potential threats and vulnerabilities

* Acceptable Use Policy (AUP) and policy enforcement:

Coverage: The AUP sets clear guidelines regarding the downloading and sharing of copyrighted content, which addresses the risk of unauthorized downloading. However, enforcement of the policy could be improved to prevent violations.

* Web filtering and firewall solutions:

Coverage: Implementing web filtering and firewall solutions helps to block access to known websites facilitating illegal downloads, reducing the risk of unauthorized downloading and sharing of copyrighted content.

* Disk space monitoring tools:

Coverage: Disk space monitoring tools provide visibility into storage usage and can help identify low disk space issues. However, they may not directly address the risk of missing critical files or the underlying cause of low disk space, such as potential malware or unauthorized actions.

**Vendor recommendation:**

* Web filtering and firewall solutions: Look for reputable vendors that offer robust web filtering and firewall technologies. Consider factors such as their track record, ease of implementation, scalability, compatibility with existing infrastructure, and the ability to customize filtering rules to meet your organization's needs.
* Disk space monitoring tools: Explore vendors that provide disk space monitoring solutions with features like real-time monitoring, customizable alerts, trend analysis, and reporting capabilities. Consider solutions that integrate well with your existing systems and provide actionable insights to manage disk space efficiently.
* Email security measures: Consider vendors that offer comprehensive email security solutions, including spam filters, email authentication protocols, and anti-phishing capabilities. Look for vendors with strong threat intelligence, advanced filtering capabilities, and seamless integration with popular email platforms.

**Metrics to be monitored:**

To ensure effective control and risk management, it is important to monitor relevant metrics that provide insights into the performance, effectiveness, and security posture of the organization

* Security Incident Metrics:

Number of security incidents reported and their classification (e.g., phishing attacks, unauthorized access, malware infections).

Mean time to detect and respond to security incidents.

Incident resolution time and closure rate.

Incident trend analysis to identify recurring patterns or emerging threats.

* Compliance Metrics:

Compliance status with relevant regulations, industry standards, and internal policies.

Number and status of compliance assessments, audits, or certifications.

Percentage of control objectives achieved.

* User Access Metrics:

User access privileges and permissions: Number of users with privileged access, accounts with excessive permissions, and orphaned accounts.

User activity monitoring: Number of anomalous or suspicious user activities detected.

User access review and recertification: Percentage of user access rights reviewed and recertified within defined intervals.

* Vulnerability Management Metrics:

Number and severity of identified vulnerabilities.

Time taken to patch or remediate vulnerabilities.

Percentage of critical vulnerabilities remediated within defined time frames.

Vulnerability scan coverage and frequency.

* Security Awareness Metrics:

Completion rate of security awareness training programs.

Performance in security awareness assessments or simulated phishing exercises.

* Feedback and survey results to measure the effectiveness of training programs.

Monitoring plan:

*Create a monitoring plan that includes:*

* *SIEM*

*Define Objectives:*

*Identify the main objectives of the monitoring plan, such as detecting and responding to security incidents, ensuring compliance with regulations, or monitoring specific systems or applications.*

*Identify Data Sources:*

*Determine the data sources to be monitored, such as network logs, system logs, application logs, firewall logs, antivirus logs, and authentication logs. Ensure that the necessary data sources are configured to send logs to the SIEM system.*

*Define Use Cases and Alerting Rules:*

*Identify specific use cases and security events to monitor. Examples include detecting unauthorized access attempts, unusual network traffic patterns, or potential malware infections. Define alerting rules in the SIEM system based on these use cases to trigger notifications or escalate incidents.*

*Configure Log Collection:*

*Set up log collection and ingestion in the SIEM system to gather data from the identified sources. Configure log collectors, agents, or syslog servers to forward logs to the SIEM system for processing and analysis.*

*Establish Baselines:*

*Establish baselines for normal system behavior, network traffic, and user activity. Use statistical analysis or machine learning techniques in the SIEM system to create baselines for different log types. Deviations from these baselines can indicate potential security incidents or anomalies.*

*Define Alert Thresholds:*

*Set appropriate alert thresholds for different types of events and anomalies. Determine the severity levels and response actions associated with each type of alert. For example, critical events may require immediate notification and response, while informational events can be reviewed periodically.*

*Incident Response and Escalation:*

*Define the incident response process and escalation procedures in alignment with the SIEM system. Specify the roles and responsibilities of the incident response team members, including incident handlers, analysts, and decision-makers. Outline the steps to be taken when an alert is triggered, from initial investigation to containment, eradication, and recovery.*

*Regular Review and Fine-tuning:*

*Conduct regular reviews of the SIEM system's performance, including the effectiveness of alerts, false positives, and false negatives. Fine-tune alerting rules, thresholds, and correlation rules to optimize the system's accuracy and efficiency.*

*Reporting and Documentation:*

*Define reporting requirements and generate regular reports based on the monitored events and incidents. Document the monitoring plan, including procedures, configurations, and any changes made over time. Maintain an inventory of assets, data sources, and their monitoring status.*

*Continuous Improvement:*

*Continuously improve the monitoring plan based on lessons learned from security incidents, industry best practices, and changes in the threat landscape. Stay updated with emerging threats, new log sources, and updates to the SIEM system itself.*

*24/7 Monitoring:*

* *Resource Allocation:*

*Determine the staffing requirements for round-the-clock monitoring. This may involve hiring dedicated security analysts or utilizing a Security Operations Center (SOC) that operates 24/7.*

* *Shift Scheduling:*

*Establish shift schedules to ensure continuous coverage. Divide monitoring responsibilities into shifts, such as day, evening, and night shifts, with overlapping hours for smooth transition and knowledge transfer.*

* *Real-time Alerting and Incident Response:*

*Configure the SIEM system to generate real-time alerts for critical events and security incidents. Define escalation procedures and establish communication channels for incident response, ensuring that the necessary personnel can be reached promptly.*

* *On-call Support:*

*Designate on-call support for after-hours incidents and emergencies. This includes having a roster of personnel available outside regular working hours who can be contacted if an incident requires immediate attention.*

* *Security Operations Center (SOC):*

*Consider establishing or outsourcing to a dedicated SOC. A SOC provides a centralized team of security experts who are trained to monitor and respond to security events on a 24/7 basis. They can leverage the SIEM system and other security tools to detect and respond to incidents effectively.*

* *Automated Response and Orchestration:*

*Implement automated response and orchestration capabilities within the SIEM system. This allows for the automation of certain incident response actions, such as blocking IP addresses or isolating compromised systems, to enable faster and more efficient response.*

* *Monitoring Redundancy:*

*Ensure monitoring redundancy by having multiple SIEM system instances or distributed monitoring points in different locations. This helps ensure continuous monitoring in case of system failures, network outages, or localized incidents.*

* *Regular Performance Monitoring:*

*Monitor the performance and health of the SIEM system itself. Implement proactive monitoring of system resources, log ingestion rates, storage capacity, and any performance bottlenecks to ensure continuous and uninterrupted operation.*

* *Training and Knowledge Sharing:*

*Provide ongoing training and knowledge sharing sessions for the security analysts involved in 24/7 monitoring. This helps keep them updated on the latest threats, techniques, and tools, and enhances their ability to identify and respond to security incidents effectively.*

* *Incident Reporting and Documentation:*

*Implement standardized incident reporting and documentation processes. Ensure that all incidents, alerts, and actions taken during 24/7 monitoring are documented accurately for post-incident analysis, compliance requirements, and continuous improvement.*

* *Remember to review and adapt the 24/7 monitoring approach as needed to align with the organization's resources, budget, and specific security requirements. Continuous monitoring and evaluation are crucial to maintain an effective and responsive security posture.*

Incident response capabilities:

* Incident Response Team:

Establish a dedicated incident response team consisting of individuals with expertise in cybersecurity, incident handling, and forensic analysis. Assign specific roles and responsibilities to team members.

* Incident Response Plan:

Develop a comprehensive incident response plan that outlines the step-by-step procedures to be followed during security incidents. Include communication channels, escalation procedures, and incident classification criteria. The plan should address various types of incidents, such as data breaches, malware infections, and social engineering attacks.

* Incident Triage and Classification:

Implement a process for promptly triaging and classifying incidents based on their severity, impact, and urgency. This allows for effective resource allocation and prioritization of incident response efforts.

* Communication and Reporting:

Establish clear communication channels for reporting and responding to incidents. Ensure that employees know how and whom to report incidents to within the organization. Implement a centralized incident reporting mechanism and define procedures for timely reporting to the appropriate stakeholders, such as management, legal counsel, and law enforcement, if necessary.

* Forensic Investigation:

Have trained personnel or engage external experts to conduct forensic investigations in response to incidents. They should be able to collect and analyze digital evidence, identify the root cause of the incident, and provide insights for remediation and prevention.

SDLC:

Enablers INC. should adopt an SDLC process that incorporates security measures and addresses the specific challenges faced by the organization. Here's a suggested SDLC process that takes into account the mentioned issues:

* Requirements Gathering:

Engage with stakeholders to gather and document software requirements, including security and compliance considerations. Clearly define acceptable internet usage policies and any restrictions on downloading unauthorized software.

* Analysis and Design:

Conduct a thorough analysis of the requirements, including security requirements. Design the software architecture, taking into account security controls and measures to prevent unauthorized activities, data breaches, and malware infections.

* Development:

During the development phase, follow secure coding practices, such as input validation, output encoding, and proper authentication and authorization mechanisms. Implement security features and controls to protect against potential vulnerabilities.

* Testing:

Perform rigorous security testing throughout the SDLC, including vulnerability assessments, penetration testing, and code reviews. This helps identify and fix security flaws and vulnerabilities before deployment

* Deployment:

Prioritize security considerations during the deployment phase. Ensure that systems are properly configured, hardened, and patched. Implement strict access controls, including least privilege principles, and consider the use of endpoint protection software.

# Learnings from Capstone:

*List down your learnings from the whole Capstone exercise.*

* *The importance of cybersecurity.*

*Enablers INC did not have adequate cybersecurity measures in place, which led to a data breach and the loss of critical files. This incident could have been avoided if the company had implemented stronger security measures, such as a firewall, antivirus software, and employee training on cybersecurity best practices.*

* *The importance of having clear policies and procedures*

*Enablers INC did not have clear policies and procedures in place regarding internet usage and data security. This led to confusion among employees and made it difficult for the company to respond to the data breach. The company should have developed clear policies and procedures that outline what employees can and cannot do when using the internet, as well as how to report security incidents.*

* *The importance of having a plan for responding to security incidents:*

*Enablers INC did not have a plan for responding to security incidents. This made it difficult for the company to respond quickly and effectively to the data breach. The company should develop a plan that outlines the steps that will be taken in the event of a security incident, such as notifying employees, contacting law enforcement, and restoring data.*

* *The importance of having a strong IT department:*

*Enablers INC's IT department was not adequately staffed or equipped to handle the data breach. This made it difficult for the company to investigate the incident and recover the lost data. The company should invest in a strong IT department that is staffed with qualified professionals who can help to protect the company's data and respond to security incidents.*