Project 5: Risk Management Case Study

Cyber Risk Management Plan Developed for DHA Enterprise Inc. (DHAEI)

Prepared by: Esther Ogunlana
Date: October 19, 2024

Executive Summary

This document presents a comprehensive Cyber Risk Management Plan for DHA Enterprise Inc. (DHAEI), aimed at identifying, assessing, and mitigating cybersecurity risks that could impact the organization's operations and security. As DHAEI continues to expand its software development and IT services, a structured approach to managing risks is essential to safeguarding its assets and ensuring business continuity.

The scope of this plan encompasses all operational areas, including software development, network security, and data management. Key stakeholders in this initiative include the Executive Team, the Information Security Manager, the IT Department, and all employees involved in daily operations. By adhering to NIST guidelines, particularly NIST SP 800-30, the risk assessment process involves cataloging critical assets, identifying threats and vulnerabilities, and evaluating the potential impact and likelihood of risks.

The assessment identified three primary assets: company-issued computers, File Servers, and User Data and Mapped Network Drives. Each asset presents unique vulnerabilities and threats, including malware attacks, data loss, and unauthorized access. The most significant risks identified are data loss, which poses substantial threats to the availability of DHAEI's data, and malware attacks, which can compromise confidentiality and integrity.

To address these threats, we recommend specific treatment strategies:

1. Malware Attacks: Implement advanced endpoint protection solutions, conduct regular employee training, ensure timely software updates, and utilize network segmentation.
2. Data Loss: Establish a robust backup strategy, employ data encryption, enforce strict access controls, and develop an incident response plan.
3. Unauthorized Access: Enforce multi-factor authentication, conduct regular security audits, implement role-based access control, and establish continuous monitoring and logging of access attempts.

By adopting these recommendations, DHAEI will significantly enhance its cybersecurity posture, mitigate potential risks, and ensure the integrity and availability of its critical assets.

Purpose, Scope, and Users

A cyber risk management plan is a systematic strategy for prioritizing potential threats within an organization. It encompasses the processes of identifying, analyzing, assessing, and mitigating cybersecurity risks (Firch, 2024).

This document will identify and mitigate risks that may impact DHAEI's operations and security. The scope encompasses all operational areas within DHAEI, including software development, network security, and data management. Key users of this plan are the Executive Team, Information Security Manager, IT Department, and all employees involved in daily operations.

Risk Assessment Process

The risk assessment process will follow the guidelines set by NIST SP 800-30, which outlines a structured approach to identifying, assessing, and prioritizing risks (NIST, 2012). The process will involve:

1. Identifying Assets: Cataloging all critical assets within DHAEI, including servers, software, and data.
2. Identifying Threats and Vulnerabilities: Assessing potential threats to each asset, such as cyberattacks, data breaches, and natural disasters.
3. Determining Risk Levels: Evaluating the likelihood and potential impact of identified risks.
4. Identifying Involved Users/Groups: Assessing potential users based on the identified assets.

Assets, Vulnerabilities, and Threats

DHAEI operates in a complex environment with various high-level and low-level assets. In this report, we will examine one asset from each of the security categories. Specifically, we will focus on user devices under technical requirements, file servers under security requirements, and user data under user requirements.

1. User Devices

DHAEI has about 1500 users in the main office who use desktop computers, 200 users in the branch office, and 20 programmers who work from home. Any of these devices can become an entry point for threat actors to gain access to DHAEI.

Potential Threats

- Malware Attacks: Company-issued computers are vulnerable to various types of malware, including ransomware, which can encrypt files and demand payment for decryption (NVD, 2023).
- Phishing Attacks: Employees may inadvertently click on malicious links or attachments received in emails, leading to credential theft or malware installation.

Potential Vulnerabilities

- Unpatched Software: Outdated operating systems or applications can have known vulnerabilities that attackers exploit (NVD, 2023).
- Weak Passwords: Poor password practices can lead to unauthorized access.

File Servers

DHAEI's existing environment has servers that service the main and branch offices. The main office servers, Domain Controllers (DCI and DC2), File Server (FSI), Windows Software Update Services (WSUS) Server (WSUSI), Infrastructure Server (DHADNS), and Read-Only Domain Controllers (RODC) in each branch office.

Potential Threats

- Unauthorized Access: File servers can be targeted by attackers seeking to gain access to sensitive data, especially if access controls are weak.
- Data Breaches: If sensitive data is not adequately protected, it can be exposed during a cyber incident or accidental leak (NVD, 2023).

Potential Vulnerabilities

- Improper Configuration: Misconfigurations in security settings can leave file servers exposed to attacks (NVD, 2023).
- Lack of Encryption: Data at rest not being encrypted makes it susceptible to unauthorized access in case of physical theft or breach.

2. User Data and Mapped Network Drives

Data is a very important asset to any organization. The staff at DHAEI play an enormous role in creating and managing data. User data stored on the company server, (FSI) and eventually, branch office server, and sensitive company data that needs protection from unauthorized access.

Potential Threats

- Data Loss: Data on mapped drives can be lost due to ransomware attacks or accidental deletions by users.

- Insider Threats: Employees may inadvertently or intentionally compromise data security, leading to data leaks or unauthorized access.

Potential Vulnerabilities

- Insufficient Backup: Without regular backups, user data on mapped network drives is at risk of being permanently lost or deleted due to hardware failures or cyber incidents (NVD, 2023).
- Access Control Weaknesses: Poorly managed access permissions can lead to unauthorized access to sensitive user data.

Determining the Risk Owners

Risk ownership does not fall on a single person in an organization. For DHAEI, several users and roles are involved in managing and mitigating the identified threats. Their collective efforts help to create a secure environment and ensure that DHAEI can effectively respond to potential risks.

1. End Users (Employees)

- Role: General employees who use company-issued computers and access file servers.
- Involvement: Responsible for following security protocols, such as recognizing phishing attempts and using strong passwords.
- Can inadvertently introduce threats if they engage in unsafe online behaviors or fail to report suspicious activities.

2. IT Security Team

- CISO (Paul Alexander)
- Role: Oversees the overall security strategy and incident response.
- Involvement: Establishes policies for securing endpoints and file servers, and ensures compliance with security standards.
- Security Technicians (e.g., Harold Fry)
- Role: Implement day-to-day security measures and monitor for threats.
- Involvement: Regularly update software, conduct security audits, and respond to incidents.

3. IT Support Staff

- Help Desk Technicians (e.g., Carlos Mendez, Tina Witherly)
- Role: Provide support for technical issues and user queries.
- Involvement: Assist employees in resolving security-related issues, such as malware infections, and educate users on safe practices.

4. Network Administrators

- Senior Network Admin (Tina Mann) and Network Architects (Vincent DiSalvo):
- Role: Manage the network infrastructure and ensure secure configurations.
- Involvement: Monitor network traffic for unusual activity, maintain access controls, and ensure proper configuration of servers.

5. Data Owners

- Manager of Corporate Security (Robert Briscoe):
- Role: Responsible for data protection policies and compliance.
- Involvement: Defines access controls for sensitive data and ensures that data protection measures are in place.

6. Executive Leadership

- CIO (Amanda Wilson) and CEO (Alan Hake):
- Role: Set the strategic direction for IT and security initiatives.
- Involvement: Allocate resources for security measures and support the overall security culture within the organization.

Impact and Likelihood

Threat	Impact	Likelihood	Confidentiality, Integrity, and Availability Impact
Malware Attack	8	3	A malware attack would have a high impact on Confidentiality, Integrity, and Availability but has a lower likelihood of happening.

Unauthorized Access	9	2	A potential data breach would have a significant impact on Confidentiality, and Integrity but the likelihood depends on security measures that have been put in place.
Data Loss	9	4	Data loss would have a higher impact on Availability due to permanent loss of critical user data.

Risk Acceptance Criteria

The most likely and highest risk item is Data Loss as it poses significant threats to the availability of DHAEI's data. Given the current threat landscape, this risk cannot be ignored. Other items may be minimized based on their lower likelihood and impact, allowing the organization to allocate resources effectively toward higher-priority risks (NIST, 2020)

Risk Treatments

1. Malware Attack

Recommended Treatment

- Endpoint Protection: Implement advanced endpoint protection solutions that include antivirus, anti-malware, and behavioral analysis to detect and block malware before it can cause harm (NIST SP 800-83).
- User Education and Training: Conduct regular training sessions to educate employees about phishing tactics and safe browsing practices. Awareness programs can reduce the likelihood of malware infection (NIST SP 800-50).
- Regular Software Updates: Ensure that all company-issued computers are regularly updated with the latest security patches and software updates to mitigate vulnerabilities that could be exploited by malware (NVD, 2023).
- Network Segmentation: Utilize network segmentation to limit the spread of malware if an infection occurs. This can isolate critical systems from infected endpoints (MITRE ATT&CK: T1573).

2. Data Loss

Recommended Treatment

- Regular Backups: Implement a robust backup strategy that includes regular backups of user data to secure offsite locations. Utilize both full and incremental backups to ensure data can be restored after loss (NIST SP 800-34).
- Data Encryption: Encrypt sensitive data both at rest and in transit to protect it from unauthorized access and loss during incidents (NIST SP 800-111).
- Access Controls: Implement strict access controls and permissions for users accessing sensitive data. This reduces the likelihood of accidental deletion or unauthorized access (NVD, 2023).
- Incident Response Plan: Develop and regularly test an incident response plan to ensure swift action in case of data loss events, minimizing recovery time and impact (MITRE ATT&CK: IR).

3. Unauthorized Access

Recommended Treatment

- Multi-Factor Authentication (MFA): Enforce MFA across all systems to add an extra layer of security beyond just passwords, making unauthorized access more difficult (NIST SP 800-63).
- Regular Security Audits: Conduct periodic security audits and vulnerability assessments to identify and remediate potential weaknesses in access controls (NVD, 2023).
- Role-Based Access Control (RBAC): Implement RBAC to ensure users have access only to the data necessary for their roles, minimizing unnecessary exposure (NIST SP 800-162).
- Monitoring and Logging: Establish continuous monitoring and logging of access attempts to detect and respond to suspicious activity in real-time (MITRE ATT&CK: T1071).

Conclusion

The Cyber Risk Management Plan developed for DHAEI outlines a proactive approach to identifying and addressing potential cybersecurity threats. The detailed risk assessment has illuminated vulnerabilities associated with key assets, allowing the organization to prioritize its risk management efforts effectively.

The recommended treatments focus on enhancing existing security measures and fostering a culture of security awareness among employees. As DHAEI continues to grow, maintaining robust cybersecurity practices will be vital in protecting sensitive data and ensuring operational resilience. By implementing these strategies, DHAEI can not only safeguard its assets but also build trust with its clients and stakeholders, reinforcing its position as a leader in the software development industry. This plan is a crucial step toward achieving a secure and efficient operational environment, ultimately contributing to the organization's long-term success.

References

Firch, J. (2024, May 19). *How to develop a cyber risk management plan*. PurpleSec. https://purplesec.us/learn/cyber-risk-management-plan/

MITRE ATT&CK. (n.d.). *MITRE ATT&CK framework*. Retrieved from https://attack.mitre.org/

National Institute of Standards and Technology (NIST). (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30). U.S. Department of Commerce. Retrieved from https://doi.org/10.6028/NIST.SP.800-30

National Institute of Standards and Technology (NIST). (2020). *Framework for improving critical infrastructure cybersecurity* (NIST Special Publication 800-53). U.S. Department of Commerce. Retrieved from https://doi.org/10.6028/NIST.SP.800-53

National Institute of Standards and Technology (NIST). (2023). *National vulnerability database*. Retrieved from https://nvd.nist.gov/

National Institute of Standards and Technology (NIST). (n.d.). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53). U.S. Department of Commerce. Retrieved from https://doi.org/10.6028/NIST.SP.800-53