Risk Management Case Study for DHAEI

By
Victor Onukwu

Table of Content

Executive Summary

DHAEI, a software development company, is planning to expand by opening a new branch office in Brampton, Mississauga. To ensure a smooth expansion and maintain security, the company has created a Risk Management Plan that covers technical, security, and user requirements.

Case Overview:
DHAEI is a well-known player in the internet access and web hosting industry, founded in 2019 and led by CIO Amanda Wilson and Chief Information Security Paul Alexander. The company has invested around $500,000 in equipment, personnel, and training to demonstrate its commitment to security and integrity as it grows into new locations.

Risk Assessment and Identification:
In this particular context, my assessment of potential risks has identified three main areas of concern:

1. Cyber Security Threats and Data Breaches: The possibility of data breaches and unauthorized access.

2. Network and Bandwidth Efficiency: Ensuring that data transfer is efficient, especially for remote workers.

3. Hardware and Server Monitoring: The need for effective central monitoring and notification of hardware events.

Based on my assessment, these risks have different levels of impact and likelihood, with security threats being the highest priority.

Recommendations for Risk Treatment:

1. Cyber Security Threats and Data Breaches (High Priority):
- Implement strong encryption and access control measures.
- Use industry-standard encryption protocols like AES.
- Enforce access control to prevent unauthorized access.
- Develop a comprehensive strategy to deter theft and protect hardware and servers.

2. Network and Bandwidth Efficiency (Moderate Priority):
- Utilize a content delivery network (CDN) to reduce VPN traffic.
- Employ data compression techniques for efficient data transfer.
- Monitor and optimize bandwidth to improve network efficiency.

3. Hardware and Server Monitoring (Low Priority):

- Implement server monitoring software to promptly detect hardware events.
- Configure alert systems and email notifications for hardware events.
- Regularly update and maintain server monitoring tools.

DHAEI can effectively manage risks and protect data security by implementing these recommendations, which are in line with industry standards and prioritize risk management.

This Risk Management Plan enables DHAEI to succeed in a constantly changing industry by addressing technical, security, and user needs for the new branch office. DHAEI's commitment to secure and efficient operations is highlighted through this approach, setting the foundation for sustainable growth and success.

Purpose, Scope, and Users

The aim of this Risk Management Plan is to aid DHAEI in identifying and handling risks related to its network infrastructure and security needs. The plan's scope encompasses technical, security, and user requirements, with a focus on the new branch office in Brampton, Mississauga. The primary individuals who will utilize this plan are the CIO, Amanda Wilson, Chief Information Security, Paul Alexander, and the support technicians in branch offices.

Risk Assessment and Risk Treatment Methodology:

Risk Assessment:

The Process:

The risk assessment process will involve collaboration among various stakeholders (individuals and groups) to ensure a comprehensive evaluation of potential risks. The following individuals or groups will be involved:

- Alan Hake who is the founder and Chief Executive Officer(CEO), holds overall reponsibility, and maintains strategic alignment with organizational goals,
- Amanda Wilson serves as the Chief Information Officer(CIO), responsible for overseeing the entire risk management process, providing resources, making informed decisions, and ensuring senior management buy-in.
- As the Chief Information Security Officer(CISO), Paul Alexander leads the assessment of security-related risks, vulnerabilities, and mitigation strategies.
- Technical Department: To provide insights into technical issues, updates, and network infrastructure.
- Branch Office Technicians: To offer insights into local maintenance, access control, and replication requirements.
- Security Department: To assess security risks and measures.

Assets, Vulnerabilities, and Threats

DHAEI has provided information indicating three primary threats and challenges:

1. Cyber Security Threats and Data Breaches: Ensuring the adequate protection of data against theft and unauthorized access, particularly in the event of server or drive theft.

2. Network and Bandwidth Efficiency: Minimizing VPN traffic for remote users and ensuring efficient data transfer.

3. Hardware and Server Monitoring: Implementing centralized monitoring of all servers and generating notifications for hardware events.

The following are know vulnerabilities associated with some assets identified in DHAE infrastructureI:

CVE-2021-34527 (PrintNightmare Vulnerability):
CVSS Score: 8.8 (High)
Vulnerability Description: This vulnerability in the Windows Print Spooler service could lead to privilege escalation and unauthorized access. Given that the case study mentions the use of Windows 10 on client machines, this vulnerability could impact these systems.

Mitigation: Implement the necessary security updates for the Windows Print Spooler service.

CVE-2019-0708 (BlueKeep Vulnerability):
CVSS Score: 9.8 (Critical)
Vulnerability Description: BlueKeep is a critical remote code execution vulnerability that affects Windows operating systems. The case study mentions Windows Server 2019 on the main office's domain controllers, and this vulnerability could potentially pose a significant security risk.
Mitigation: Ensure that the Windows servers are updated with the relevant security patches.

CVE-2020-1472 (Zerologon Vulnerability):
CVSS Score: 10.0 (Critical)
Vulnerability Description: This vulnerability could allow an attacker to gain unauthorized access to Active Directory domain controllers. Considering that the case study mentions a single Active Directory domain named DHA.com, this vulnerability could pose a significant threat to network security.
Mitigation: Ensure that the domain controllers are updated and follow best practices for securing Active Directory.

CVE-2020-0601 (Windows CryptoAPI Vulnerability):
CVSS Score: 10.0 (Critical)
Vulnerability Description: This vulnerability impacts Windows CryptoAPI and could enable attackers to spoof digital certificates and conduct man-in-the-middle attacks, potentially affecting the integrity of secure communications.
Mitigation: Ensure that all Windows systems, including Windows Server 2019 and Windows 10 clients, are updated to address this vulnerability.

CVE-2021-24086 (Microsoft Exchange Server Remote Code Execution Vulnerability):
CVSS Score: 9.8 (Critical)
Vulnerability Description: This vulnerability in Microsoft Exchange Server could allow an attacker to execute arbitrary code remotely. Given the case study's mention of a Windows Software Update Services (WSUS) server named WSUSI, this vulnerability could impact server security.
Mitigation: Ensure that Microsoft Exchange Server and related systems are up to date with the latest security patches.

Determining Risk Owners

For each of these risks, a chain of ownership is established:

1. Cyber Security Threats and Data Breaches: The Security Technician (Ground Level) reports to the Chief Information Security Officer (Paul Alexander), who in turn reports to the CIO (Amanda Wilson). The Security Technician is responsible for local security measures, Paul Alexander oversees information security, and Amanda Wilson maintains overall organizational oversight.

2. Network and Bandwidth Efficiency: The Technical Department (Ground Level) reports to the CIO (Amanda Wilson). The Technical Department is responsible for managing technical issues, while Amanda Wilson maintains overall oversight.

3. Hardware and Server Monitoring: The Technical Department (Ground Level) reports to the CIO (Amanda Wilson). The Technical Department handles technical aspects, while Amanda Wilson maintains overall oversight.

Impact and Likelihood Assessment

In line with the International Organization for Standardization(2022), ISO/IEC 27001:2022 For each of the three identified risks, an assessment has been conducted on their impact and likelihood:

1. Cyber Security Threats and Data Breaches:
   Impact: It has a high impact (9) on Confidentiality (C), a moderate impact (9) on Integrity (I), and a low impact (8) on Availability (A).
   Likelihood: It is Highly likely (4).

2. Network and Bandwidth Efficiency:
   Impact: It has a Moderate impact (6) on Confidentiality (C), a moderate impact (5) on Integrity (I), and a low impact (6) on Availability (A).
   Likelihood: It is moderately likely ()

3. Hardware and Server Monitoring:
   Impact: It has a Moderate impact (6) on Confidentiality (C), a moderate impact (5) on Integrity (I), and a low impact (5) on Availability (A).Likelihood: Likely (2).

Asset	Threat	Vulnera	Risk	Impact(	Likeliho	Risk(I+

		bility	**Owner**	**1-10)**	**od(1-5)**	**L)**
Database Server	Unauthorized login	Weak password ,Unpatched system	CIO-Amanda	9	4	13
VPN	Poor bandwidth efficiency	Bandwidth overuse	CIO-Amanda	6	4	10
File Server	Insider threat	Poor Monitoring	CIO-Amanda	6	2	8

Risk Acceptance Criteria

The risk with the highest likelihood, which is security threats and data breaches, can have a significant impact on DHAEI's data protection, especially in the event of server or drive theft. This risk should not be ignored or minimized, and appropriate mitigations should be implemented. The other risks can be addressed based on their potential consequences and the availability of resources.

Risk Treatment

To effectively Mitigate Security Threats (high priority):

- It is highly recommended to implement robust encryption, access control mechanisms, and regular data backup measures.
- It is crucial to utilize industry-standard encryption protocols like AES to ensure the utmost protection of sensitive data.
- Additionally, the implementation of access control lists will help restrict unauthorized access, further enhancing the overall security posture.
- To deter theft and safeguard hardware and servers, a comprehensive theft-deterrence strategy should be put in place.

Mitigation for optimal Network performance and Bandwidth Efficiency (moderate priority):

- It is strongly advised to consider implementing a content delivery network (CDN). By leveraging a CDN, VPN traffic can be minimized, resulting in improved network efficiency.
- Furthermore, the use of data compression techniques can significantly enhance data transfer efficiency.
- To ensure ongoing network optimization, it is essential to deploy bandwidth monitoring and optimization tools.

Mitigation in terms of Hardware and Server Monitoring (Moderate priority):

- It is recommended to implement dedicated server monitoring software. This software will enable the detection of hardware events, allowing for timely response and troubleshooting.
- To stay informed about any hardware events, it is crucial to configure alerts and email notifications.
- Regular maintenance and updates of the server monitoring tools are also necessary to ensure their effectiveness.

Priority and Rationale

The priority levels are assigned based on the potential impact and likelihood, ensuring a balanced approach to risk management. By implementing the recommendations mentioned, DHAEI can effectively manage the identified risks and optimize its network infrastructure while ensuring data security. These measures are in alignment with industry standards and best practices for information security and network efficiency. .

Conclusion

In order to maintain a secure IT environment, DHAEI must keep a close eye on CVE databases and regularly apply security patches and updates to address any vulnerabilities. It is also recommended to implement ISO 27001 and NIST standards, along with a comprehensive vulnerability management program and periodic security assessments to proactively identify and mitigate potential threats. This Risk Management Plan provides DHAEI with a framework to meet the technical, security, and user requirements for the new branch office. By systematically identifying, assessing, and mitigating risks, DHAEI can ensure the security and efficiency of its network infrastructure and meet its user and security requirements.

References

National Institute of Standards and Technology. (2023, October 17). Vulnerabilities search and statistics. https://nvd.nist.gov/vuln/search

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html

Lighthouse Labs. (2022). Project: Risk Management Case Study. https://www.lighthouselabs.ca/compass/projects/risk-management-case-study

ACME INC. (2021). Sample risk management methodology document. https://www.lighthouselabs.ca/compass/projects/risk-management-case-study