SCOTT
MACLEAN

NOVEMBER 2024

# RISK MANAGEMENT PLAN

# DHA ENTERPRISE INC.

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

DHA Enterprise Inc is a software development company that provides internet and web hosting services. The company requires a comprehensive risk management strategy to protect is spread out infrastructure and sensitive data. Our assessment has identified severe risks related to data security, system availability and access control across it's many offices.

We recommend implementing enhanced authentication processes, establishing robust data encryption protocols and to strengthen business continuity measures. Priority has been given to customer data protection and keeping services online while accommodating for the companies expansion to Brampton.

# PURPOSE, SCOPE, USERS

## Purpose

To identify, assess, and mitigate potential risks to DHAEI's information systems, infrastructure, and business operations while maintaining availability to customers.

## Scope

All DHAEI locations (main office and branch offices)

Cloud infrastructure (Rackspace and AWS)

Network infrastructure and authentication systems

Remote access systems

Data storage and transmission systems

## Users

Executive management team

IT security team

Branch office support technicians

Remote workers

System administrators

# INDIVIDUALS/GROUPS TO INVOLVE

Chief Information Security Officer (CISO) - Paul Alexander

Leads risk assessment process

Provides security expertise and oversight

Coordinates between technical and management teams

Maps security controls from NIST 800-53

Branch Office Support IT

Provide insight into local infrastructure

Identify branch-specific vulnerabilities

Implement and tailor security measures locally

Cloud Infrastructure Team

Assess AWS and Rackspace security

Monitor cloud service compliance

Implement cloud security controls

Align with NIST SP 800-144 guidelines for cloud computing

# ASSETS, VULNERABILITIES & THREATS

| Risk | Mitre ATT&CK Reference | Challenges |
|---|---|---|
| Data Breach/Unauthorized Access | TA0001 - Initial Access [1]<br>TA0010 - Exfiltration | Distributed infrastructure, Remote worker access, Mixed cloud environment |
| System Availability Disruption | TA0040 - Impact [2]<br>T1498 - Denial of Service | Cloud dependencies, Branch office connectivity, Limited IT support at branch locations |
| Insider Threats | TA0004 - Priveledge escalation [3]<br>TA0005 - Defense Evasion | Branch technicians with local admin rights, Remote worker access, Password and secret management |

# DETERMINING RISK OWNERS - CHAIN OF COMMAND

## Data Breach Risk

Level 1: Security Technicians

- They have a direct responsibility for overseeing potential data breaches

Level 2: CISO

- Develops the strategies for risk mitigation

Level 3: CEO

- Oversees the entire organization

## System Availability Risk

Level 1: Support Technicians

- Monitor system performance and availability

Level 2: Infrastructure Team

- Implements disaster recovery procedures

Level 3: CIO

- Approves major system changes

## Insider Threat Risk

Level 1: HR Department

- Conducts background checks

Level 2: Security Team

- Monitors user activity

Level 3: CISO

- Develops insider threat program

# IMPACT & LIKELIHOOD

| Risk | CIA Impact | Impact Score | Likelihood |
|---|---|---|---|
| Data Breach/ Unauthorized Access | C, I | High | High |
| System Availability Disruption | A | Moderate | Moderate |
| Insider Threats | C, I, A | Moderate | Moderate |

# RISK ACCEPTANCE CRITERIA

The key factors that make Data Breach the highest scoring threat are:

1. Multiple Attack Surfaces
   - Main office in Oshawa
   - Multiple branch offices
   - New Brampton office being established
   - Each location represents a potential entry point

2. Remote Work Environment
   - Using L2TP VPN connections
   - Company-issued laptops
   - Potential for device loss/theft
   - Risk of unsecured home networks

3. Diverse Employee Base
   - 1,500 users in main office
   - 200 users per branch office
   - Remote workers
   - Branch office technicians with elevated privileges

Having Data Breach as the highest risk, some of the controls used for insider threat or system availability may be ignored based on most resource allocation and funds being put towards data breach mitigation. Things such as paying for natural disaster insurance may be too expensive to cover all the assets.

# RISK TREATMENT PLAN

## DATA BREACH RISK

Proposed Implementations:

1. Encryption for File Servers (NIST SC-28): [4]

Encrypt all sensitive data stored on file servers using a strong encryption algorithm.
Implement a robust key management system to protect encryption keys.
Regularly test encryption and decryption processes to ensure their effectiveness.

2. Enhanced VPN Security (NIST AC-17):

Implement strong authentication methods, such as multi-factor authentication (MFA).
Enforce strict access controls to limit VPN access to authorized users.
Regularly monitor VPN traffic for anomalies and potential security threats.

3. Access Control System (NIST AC-2): [5]

Implement role-based access control (RBAC) to assign appropriate permissions to users.
Regularly review and update access controls.
Enforce the principle of least privilege.
Implement strong password policies and enforce password rotation.
Monitor user activity and log all access attempts.

4. Regular Security Awareness Training (NIST SA-6):

Conduct regular security awareness training sessions for all employees.
Provide training on topics such as phishing, social engineering, and password hygiene.
Test employees' knowledge through simulated phishing attacks.

5. Incident Response Planning (NIST CP-2):

Develop and test a comprehensive incident response plan.
Identify key personnel and their roles in responding to incidents.
Establish procedures for containing and mitigating incidents.

# RISK TREATMENT PLAN

## SYSTEM AVAILABILITY RISK

Proposed Risk Treatments:

1. Implement Least Privilege Principle (NIST AC-6):
Grant users only the minimum necessary permissions to perform their job functions.
Regularly review and update user permissions.

2. Enforce Strong Access Controls (NIST AC-3):
Implement strict access controls for branch office users.
Limit access to sensitive systems and data to authorized personnel.
Monitor and log user activity in branch offices.

3. Minimize Local Administrative Rights (NIST AC-3):
Implement granular data access controls to restrict access to sensitive data.
Use data loss prevention (DLP) solutions to prevent unauthorized data transfer.

4. Control Mapped Drive Access (NIST AC-3):
Configure Office 365 security settings to protect against unauthorized access.
Implement multi-factor authentication (MFA) for Office 365 accounts.
Use advanced threat protection features to detect and block malicious attacks.

5. Secure Cloud Access (NIST AC-17):
Implement strong access controls for cloud-based resources.
Use cloud access security broker (CASB) solutions to monitor and control cloud usage.

# RISK TREATMENT PLAN

## INSIDER THREAT RISK

Proposed Implementations and Corresponding NIST Controls: AC-6

1. Least Privilege Implementation:

Enforce the principle of least privilege.

2. Branch Office Access Restrictions AC-3 Access Control

Implement strict access controls for branch office users.

3. Local Maintenance Rights: AC-3

Minimize local administrative rights on workstations.

4. Data Access Controls: AC-3

Implement granular data access controls.

7. Office 365 Security: AC-17 Remote Access

Configure Office 365 security settings.

Implement multi-factor authentication.

Use advanced threat protection features.

# CITATIONS AND REFERENCES

1. Initial access. Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/tactics/TA0001/

2. Impact. Impact, Tactic TA0040 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/tactics/TA0040/

3. Privilege escalation. Privilege Escalation, Tactic TA0004 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/tactics/TA0004/

4. Protection of information at rest - CSF tools. CSF Tools - The Cybersecurity Framework for Humans. (2021b, March 5). https://csf.tools/reference/nist-sp-800-53/r4/sc/sc-28/

5. Account management - CSF tools. CSF Tools - The Cybersecurity Framework for Humans. (2021a, May 29). https://csf.tools/reference/nist-sp-800-53/r4/ac/ac-2/