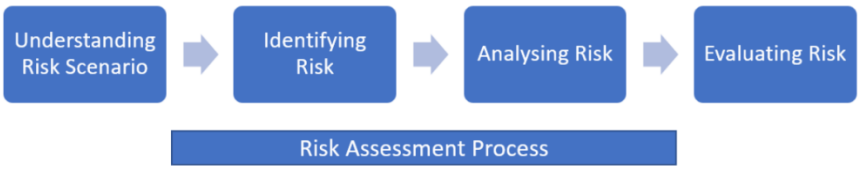
PROJECT WEEK 5 DAY 2: Risk Management Plan for DHA Enterprise Inc. (DHAEI)

Submitted by: Navneet Kaur

RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY

1. **Purpose, scope, and users:**
   The purpose of this document is to define the methodology for assessment and treatment of information risks in DHAEI, and to define the acceptable level of risk according to the ISO 270001 as well as NIST standard.
   It would be applied to assets of the company DHAEI, all branches and users which could have an impact of information security within the ISMS.
   Users are all employees, upper management CEO, senior officers CISO, supervisors and customers who access the internet for small office/home office (SOHO).
2. **Risk Assessment and Risk Treatment Methodology**
   The process:
   Risk Assessment is implemented through the Risk Assessment Table. The Risk Assessment process is coordinated by the information security analyst, identification of threats and vulnerabilities is performed by asset owners, and assessment of consequences and likelihood is performed by risk owners. DHAEI in selective situations will have the same asset owner and risk owner for a given asset.
   So three groups are:
   - Head of departments and management
   - Assets owners
   - Risk owners(risk management teams)

   The Risk assessment table:
   https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C5/Cyber+BC+C5.1/Asset+Table+Example.pdf



Assets, Vulnerabilities, and Threats
ASSETS:
Hardware: computers, laptops, printers, scanners, servers, network equipment, storage media)
Software: application software: word, spreadsheets, database manages, emails) all cloud based, OS, Websites, ERP, driver software
People (employees (IT security teams) , customers and management (CEO, CISO)
Information in electronic form
Infrastructure warehouses, building, ups devices, power generator, cables, HVAC equipment, physical security systems

Outsources services: electrical power supply, internet providers, information system maintenance, mail and courier services

Threats:

Cyber Threats:

Phishing Attacks: Cybercriminals may use deceptive emails, messages, or websites to trick customers or employees into divulging sensitive information like login credentials or payment details.

Malware and Ransomware: The DHAEI business could be targeted by malware or ransomware, leading to data encryption, theft, or system disruption.

Man-in-the-Middle Attacks: Attackers intercept communication between the DHAEI website and customers, potentially stealing sensitive data during transactions.

SQL Injection and Cross-Site Scripting (XSS): Poorly secured web applications may be vulnerable to these attacks as DHAI has huge Database having different branches in province, allowing hackers to access the database or manipulate website content.

Credential Stuffing: Cybercriminals attempt to log in using stolen username-password combinations from other data breaches, hoping that users reuse passwords.

Data Breach:

Customer Information Exposure: If customer data like names, addresses, payment details, and purchase histories are compromised, it could lead to identity theft and financial losses for customers.

Legal and Regulatory Consequences: Data breaches may result in legal actions, fines, or penalties due to non-compliance with data protection regulations.

Reputational Damage: A data breach can severely harm the reputation of the DHAEI business, leading to loss of customer trust and loyalty.

Supply Chain Risks:

Third-Party Vulnerabilities: Cyber attackers may target third-party vendors or suppliers connected to the internet provider business, using them as a point of entry into the business's network.

Counterfeit Products: Supply chain compromises can lead to counterfeit products being sold on the DHAIE website, damaging the business's reputation and customer trust.

Data Integrity: If the supply chain data is manipulated or compromised, the e-commerce business may face inventory and logistics challenges.

Vulnerabilities:

Vulnerabilities to Cyber Threats:

Lack of Email Security: Insufficient email security measures can make the business susceptible to phishing attacks, where employees and customers may unknowingly click on malicious links or disclose sensitive information.

Outdated Software: Failure to keep software up to date, including operating systems, web browsers, and plugins, may expose the website to known vulnerabilities that cybercriminals can exploit.

Inadequate Network Security: Weak network security measures, such as open ports or lack of firewalls, could allow unauthorized access to the DHAEI business's internal systems.

Insufficient Web Application Security: Web applications with improper input validation and weak coding practices may be vulnerable to SQL injection, cross-site scripting (XSS), and other web based attacks.

Vulnerabilities to Data Breach:

Poor Data Encryption: Data transmitted or stored without proper encryption can be easily intercepted by attackers, potentially leading to unauthorized access and data breaches.

Insecure Data Storage: Storing sensitive data without robust security measures can expose it to theft in case of a cyberattack or unauthorized access.

Weak Access Controls: Insufficient access controls on databases and sensitive information may allow unauthorized users to view, modify, or extract critical data.

Insider Threats: Lack of monitoring and access controls can lead to insider threats where employees or privileged users misuse their access to sensitive data.

Theft/Loss: This could be the main threat for DHAEI's desktop computers & laptops.

Vulnerabilities to Supply Chain Risks:

Lack of Vendor Assessment: Failing to conduct thorough security assessments of third-party vendors could lead to partnering with suppliers with inadequate cybersecurity measures.

Unsecured Communication Channels: Communication channels with suppliers that lack encryption may expose sensitive supply chain data to interception or manipulation. Supply

Chain Complexity: A complex supply chain with multiple partners can introduce additional points of vulnerability, increasing the potential for cyber threats.

Counterfeit Product Detection: Inadequate measures to detect counterfeit products may result in unknowingly selling counterfeit goods on the platform.

Determining the risk owners:

CYBER THREATS: Chief information security officer or chief technology officer

Responsibilities:

- Developing and implementing cybersecurity policies, procedures, and best practices.
- Overseeing the implementation of security measures to protect against cyber threats.
- Monitoring and analyzing security incidents, including phishing attempts and malware attacks.
- Conducting security awareness training for employees to improve the organization's overall security posture.
- Collaborating with IT teams to ensure timely patching and updating of software and systems.

DATA BREACH: Data protection officer or chief privacy officer

Responsibilities:

- Ensuring compliance with data protection regulations and internal data handling policies.
- Implementing data encryption and access control measures to protect sensitive customer information.
- Overseeing data breach prevention and response strategies, including incident response planning.
- Collaborating with legal and compliance teams to address legal and regulatory consequences of data breaches.
- Conducting regular risk assessments to identify vulnerabilities and weaknesses in data handling processes.

SUPPLY CHAIN RISKS: Supply chain manager or chief procurement officer

Responsibilities:

- Assessing and managing risks associated with third-party vendors and suppliers.
- Implementing a vendor assessment and due diligence process to evaluate cybersecurity practices of partners.
- Establishing contractual obligations and security requirements for vendors.
- Monitoring and auditing suppliers' security practices to ensure ongoing compliance.
- Collaborating with relevant stakeholders to address supply chain complexities and potential risks

THEFT/LOSS: Users& programmers

- Users and employees have responsibility to keep their assets secure as well as company should have proper physical security teams employed in organization

Impact and likelihood:

IMPACT

High impact	10	Loss of CIA has considered, reputational damage
Moderate impact	5	Denial of services on DHAEI services like internet connection of

		their usage , website ha latency at some times of the day, DDOS attack
Low impact	0	Loss CIA doesn't affect much in cash flow , data breach and reputation

LIKELYHOOD:

High likelihood	5	Existing security controls are low or ineffective.
Moderate likelihood	3	Security controls are moderate, new incidents can be possible but not highly likely
Low likelihood	0	Existing security controls are strong and can fight against attacks.

Risk acceptance criteria:
Values 0, 1, and 2 are acceptable risks
Risk Treatment:
Risk Treatment is implemented through the Risk Treatment Table, by copying all risks identified as unacceptable from the Risk Assessment Table. Risk Treatment is conducted by the risk owner.

One or more treatment options must be selected for risks valued 10 and 5, 3

- Selection of security control or controls from Annex A of the ISO/IEC 27001 standard or some other security controls.
- Transferring the risks to a third party (e.g., by purchasing an insurance policy or signing a contract with suppliers or partners).
- Avoiding the risk by discontinuing a business activity that causes such risk.
- Accepting the risk. This option is allowed only if the selection of other Risk Treatment options would cost more than the potential impact should such risk materializes.

The selection of options is implemented through the Risk Treatment Table.
Usually, option one is selected: selection of one or more security controls. When several security controls are selected for a risk, then additional rows are inserted into the table immediately below the row specifying the risk.
In the case of option one (selection of security controls), it is necessary to assess the new value of consequence and likelihood (residual risk) in the Risk Treatment Table, in order to evaluate the effectiveness of planned controls.

Risk treatment refers to the strategies and actions taken to manage and mitigate the identified risks. For the scenarios of cyber threats, data breach, and supply chain risks in DHAEI, the risk treatment options can include the following:
Risk Treatment for Cyber Threats:
Implement Robust Cybersecurity Measures: This includes deploying firewalls, intrusion detection systems, and antivirus software to protect against various cyber threats like malware, phishing, and DDoS attacks.
Regular Security Updates and Patch Management: Ensuring that all software, including operating systems, applications, and plugins, are up-to-date with the latest security patches to fix known vulnerabilities.
Security Awareness Training: Conducting regular cybersecurity training for employees to educate them about common cyber threats, social engineering tactics, and best practices for secure online behavior.

Multi-Factor Authentication (MFA): Enforcing MFA for accessing sensitive systems or accounts to add an extra layer of protection against unauthorized access.

Risk Treatment for Data Breach:

Encryption and Access Controls: Implementing strong encryption for sensitive data, both in transit and at rest, and setting up strict access controls to limit data access to authorized personnel only.

Incident Response Plan: Developing and regularly updating an incident response plan to ensure a swift and coordinated response to data breaches, including steps for containment, eradication, and recovery.

Data Privacy Compliance: Ensuring compliance with relevant data protection regulations and industry standards to safeguard customer data and avoid legal and regulatory consequences.

Risk Treatment for Supply Chain Risks:

Vendor Assessment and Due Diligence: Conducting thorough security assessments of third-party vendors and suppliers before entering into partnerships to ensure they have adequate cybersecurity measures in place.

Contractual Obligations: Including specific security requirements and clauses in contracts with vendors to hold them accountable for maintaining a secure environment and reporting any security incidents promptly.

Continuous Monitoring: Regularly monitoring and auditing suppliers' security practices to ensure ongoing compliance with security standards and prompt identification of any deviations or vulnerabilities.

Risk Treatment for Overall Cyber Resilience:

Cyber Insurance: Consider obtaining cyber insurance to provide financial protection against potential losses resulting from cyber incidents and data breaches.

Regular Security Assessments: Conducting periodic security assessments and penetration testing to identify and address vulnerabilities before they can be exploited by attackers.

Employee Engagement: Encouraging a culture of cybersecurity awareness among employees and promoting active participation in the company's cybersecurity initiatives

All these risk treatments are aligned to NIST and ISO 27001 framework which provides all steps to identify, risk assessment, mitigation and continuous monitoring.

Executive summary

DHAEI is a private owned software development company that is Ontario based in Durham area. The company has several branches in province providing basic internet access, fast internet and web registration to small offices/home office (SOHO) individual and organizations. The company employed number of IP personnel, technical and mentors with advanced equipment which makes the $500000 of budget.it also has its own domain name i.e. DHA.com, DHAEI also a cloud based company using AWS services so that company should meet minimum level of security from attacks. I'm going to make a plan for risk assessment for this company with the knowledge of NIST and ISO 27001 framework and as well as risk assessment table link is provided in references.

CITIATIONS:

https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C5/Cyber+BC+C5.1/Asset+Table+Example.pdf
https://csrc.nist.gov/Projects/risk-management/about-rmf/select-step
https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C5/Cyber+BC+C5.2/Sub-Reading+Selecting+Controls+Part+1.pdf
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf
https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf
www.NIST.gov