**Risk management purpose for DHAEI:**

The goal is to identify and assess potential risks that could jeopardize the company’s activity. Being as proactive as possible is paramount in order to protect the assets and mitigate the risk. Lastly, having a good risk treatment strategy up to the industry best standards will provide a structured approach to protect the company’s operations, assets and reputation.

**Scope**

The scope of the Risk management plan includes all aspects of DHAEI’s operation mentioned below.

**Main office in Oshawa, Ontario with 1500 users/employees:**

DHA.com (1 Active Directory Domain)

DC1 (Domain controller 1)

DC2 (Domain controller 2)

FSI (1 File Server)

WSUS (windows software update service)

DHADNS (an infrastructure server that provides DNS services to the network)

The main office has a central technology department that is responsible for all technical issues within the company.

**Unknown amount of existing office branches (for the purpose of the assignment, we will assume 3 branches):**

RODC (one server that is configured as a read-only domain controller)

There is one support technician located in each branch office.

**20 programmers working from home:**

Connect to the main office using L2TP VPN connections.

**Planned Branch office in Brampton, Ontario:**

Data for users in the new office will be stored on FSI (server in main office)

**Risk assessment:**

Categorizing the assets mentioned in the “scope” section shows that the focus of the risk management will be aimed at the main office. The main office includes the critical infrastructures as well as the highest number of users. Also, the programmers working from home are connected to the main office network. Lastly, the planned branch office temporary server will be the FSI (file server) which is also located in the main office.

There are three individuals/groups from the company that are key to create an optimal risk management plan to help protect the main office as well as to help with opening a new branch in a safe way. Those individuals are:

1. **Paul Alexander – Chief Information Security Officer (CISO):**

* He will play an important role to protect the critical infrastructures and sensitive data of the main office by implementing security measures.
* Paul could also make sure that the security requirements for the new branch are up to industry best practices and in accord with the main office standards.

1. **Amanda Wilson -Chief information officer (CIO):**

* She has oversight over operations and strategic decisions. Her role will be important in making sure that the IT strategies align with the protection of the main office.
* She will come with strategies to successfully setup the new branch in a secure way.
* Amanda will ensure that the measures agreed upon on this plan will be incorporated into the company’s infrastructure enhancing the company’s risk management efficiency.

1. **Branch Office support technicians:**

The branch office support technicians’s input is a crucial in understanding how to duplicate their system in another branch. Also, engaging with them will give a perspective to manage and train the upcoming employee in a way that management may not have seen.

* They have insider knowledge of the company’s IT setup and operations.
* They can identify potential vulnerabilities and assist in implementing security measures.

Involving the above-mentioned key individual/group can enhanced risk management efforts to protect the main office critical infrastructure, intellectual property and data. These key players will also ensure that the process to open a new branch office in Brampton will be done in a safe way by protecting all the critical assets.

**Threats/Assets/Vulnerabilities**

1. **Data breaches and Cyber-attacks:** The constant evolution of attackers techniques make this threat even more complex to mitigate. DHAEI must protect their critical assets (listed below) from unauthorized access.

**Assets to protect:** IT infrastructure (servers, network equipment), Intellectual Property, Remote Programmers laptops, Workstations, Customer Data

**Vulnerabilities:**

* Software not updated.
* Weak Password
* Unsecured or inadequately secured remote VPN connection for remote workers.
* Human errors
* Internal attacks

1. **Disruption and Outage:** Ensuring that DHAEI activity continuity by avoiding any interruption is a challenge. Having contingency plans such as getting a Power Generator and/or an Uninterrupted Power Supply (UPS) will enable the company to swiftly recover from interruptions or prevent them altogether. In the circumstance that the main office might be experience a momentary or significant disruption the whole organization including programmers at home and branches may face significant interruption.

**Assets to protect:** Critical IT infrastructure form the main office.

**Vulnerabilities:**

* Physical damage (voluntary or not)
* Malfunction
* Power outage
* Natural disaster
* System maintenance

1. **Data loss or Data integrity issues** Ensuring that logs are properly maintained/monitored, updates are done regularly, and backups are regularly put in place is paramount in preventing permanent data loss. Relying on this one file server (FSI) poses significant risk as any failure on this file server may results in the data availability related to the intellectual property of the company and the customer data. Considering that this file server will be the temporary one for the new upcoming branch, a special attention needs to be given to this file server.

**Assets to protect:** FSI (File Server)

**Vulnerabilities:**

* Ransomware
* DDOS
* Industrial spying
* Reputation damage

**Determining the risk owners**

**Risk 1 Data breaches and Cyber-attacks:**

1. *Entry level Risk Owner: IT technicians/SOC analyst level 1 to level 3*

**Tasks**: The technician is responsible for to monitor DHAEI network and systems. He must identify the potentials threats, escalate them if need be and he must implement security measures. They play a key role in the security operations by detecting and responding to front line threats/attacks. They need to act promptly and according to security protocols.

1. *Intermediary Level Risk Owner: Chief information Security Officer (CISO) - Paul Alexander*

**Tasks**: Paul will oversee the risk management aspect and will provide guidance whenever and technician or SOC analyst has issues or when they need additional support regarding a data breach or an ongoing cyber-attack. Lastly, Paul will be responsible to communicate any recommendations to senior management.

1. *Senior Level Risk Owner: Chief Executive Officer (CEO) - Alan Hake*

**Tasks:** Holds the ultimate responsibility for the security plan and the risk for the company. Alan will be the one approving budget and strategies that Paul will submit to him.

**Risk 2 Disruption and Outage:**

1. *Entry level Risk Owner: IT technicians/SOC analyst level 1 to level 3*

**Tasks**: The operation technician is responsible for to monitor DHAEI network, systems and IT infrastructures such as servers. He must identify Hardware failures and ensuring the good functioning of the whole system components.

1. *Intermediary Level Risk Owner: Chief Information Officer (CIO)- Amanda Wilson*

**Tasks**: Amanda provides support to the operation technicians. Her role is to make sure that every day-to-day operating system and backups are functional. Her position could be to make sure that every automated system function as they should to minimize or better avoid downtime if and when they happen. Amanda will communicate with senior level executive to provide updates or to request resources to ensure the continuity of DHAEI activity with the least interruption as possible.

1. *Senior Level Risk Owner: Chief Executive Officer (CEO) - Alan Hake*

**Tasks**: Holds the ultimate responsibility for the security plan and the risk for the company. Alan will be the one responsible for making sure the business can function if no, to very little interruption. Alan will collaborate with CIO to mitigate any major interruption that may impact the DHAEI.

**Risk 3 Data loss and Data Integrity Issues:**

1. *Entry level Risk Owner: Data analyst*

**Tasks**: Responsible for data storage and integrity. DHAEI does not seem to have that specialist in house and this issue must be brought to Alan Hake attention. This would greatly improve the security of intellectual property as well as the customer’s data protection. Paul could hire one since there is a vacant position under him.

1. *Intermediary Level Risk Owner: Chief Information Officer (CIO)- Amanda Wilson*

**Tasks**: Amanda oversees the management of all the data in DHAEI. Her contribution is to set the policies, ensure compliance through data protection regulations, collaborate with the data analyst to implement the appropriate measures.

1. *Senior Level Risk Owner: Chief Executive Officer (CEO) - Alan Hake*

**Tasks**: Holds the ultimate responsibility for serious data issues. Alan must make sure that the data management strategies are created, implemented and enforced. He is to one to approve the resources needed to accomplish the above-mentioned tasks including new staff members.

**Impact and likelihood**

|  |  |  |  |
| --- | --- | --- | --- |
| Threat/Risk | CIA Potential Impact | Impact Extent (0-10) | Likelihood (0-5) |
| Data breaches & Cyber-attacks | C: High  I: High  A: Low | 8 | 4 |
| Disruption and Outage | C: Low  I: Low  A: High | 4 | 2 |
| Data Loss/Data integrity issues | C: High  I: High  A: Medium | 7 | 4 |

**Data breaches & Cyber-attacks:** A breach could lead to the leak of customers information/data (C), Unauthorized modification of intellectual property (I) and can render critical systems unavailable (A). The extent is rated at an 8 because it could significantly impact customer’s confidence towards the company and subsequently affect its reputation. The likelihood of and attack is rated at 4 because of the business activity that is mainly online and the constant evolution of threats and techniques.

**Disruption and Outage:** This threat mainly affects the availability (A) of DHAEI IT infrastructure and services. A. The extent is rated at a 4 because the mitigations are easy to implement and if the focus is on the main office, there is no reason to expect a long period of downtime if an incident occurs. The likelihood is at a 2 because proper installations and mitigations reduce the chances of an outage/disruption.

**Data loss/Data integrity issues:** If the data is lost or compromised it would impact the company’s reputation and would reduce the publics confidence in its product (C). A data loss (A) would jeopardize DHAEI intellectual property as well as the unauthorized modification of any data in the system (I). The impact is rated at a 7 because at this point in time, the new branch will be using the FSI server (until it gets its own) and therefore will not limit the server’s usage only to the main office. The likelihood would have been at 2 provided that the FSI server would have been limited to the main office usage. Because of the temporary accommodation for the new branch in Brampton, the likelihood will be considered a 4 until the FSI server returns to its main role.

**Risk acceptance criteria**: Based on the assessment of the three above mentioned threats and the assets of DHAEI, the only acceptable risk out of the three would be the Disruption and Outage. This threat does not impact the company’s reputation as much as a data loss or a cyber-attack. Also, if the company puts back up generators and UPS in place the damage done would greatly be reduced.

**Mitigations**

**Data breaches & Cyber-attacks:**

* Implement a Multi Factor Authentication
* Update the software regularly (be aware that some updates may create other vulnerabilities)
* Provide regular training to the staff members to raise awareness on social engineer threats and phishing attacks.

**Disruption and Outage:**

* Develop a disaster recovery plan and regular tests to verifying the effectiveness of the system.
* Implement real time monitoring, alerts and logs to ensure a prompt response.

While disruption would impact the organization, the impact of such an incident would be less damageable than other threats. If DHAEI puts in place regular audits, logs, back up generator and a UPS the risk would be significantly reduced.

**Data loss/Data integrity issues:**

* Implement backups regularly.
* Implement rigorous access control.
* Have regular audits and identify weaknesses and vulnerabilities.

**Mitigation Summary:**

Mitigations were based on the industry best standards framework (such as ISO 27001) to ensure a comprehensive protection of DHAEI. Applying this risk management plan would enhance DHAEI overall defense against external and internal threats and would better protect it’s assets and stakeholders interests.

**Conclusion**:

The risk management developed for DHAEI identifies the main threats the company faces and proposes effective strategies for risk mitigation. Some IT infrastructures were prioritized over others to protect the assets and the stakeholders interests. Industry best standard such as NIST and ISO 27001 have been implemented to ensure an optimal standard of protection. The involvement of key individual in DHAEI will ensure a cohesive and collaborative approach to allow a prompt response to any situation. DHAEI can pursue its activities knowing that the proper safeguards have been put in place.

**References:**

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf>

<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf>

<https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf>

<https://www.youtube.com/watch?v=PIxoHM_EJUU>