**Risk Management Case Study**

**Project**

**Student: Ismail Yasin**

**8/02/2024**

**Lighthouse Labs**

**Table of Contents**

Purpose, Scope and Users…………………………………………………………….………………………………………….Page 3  
Risk assessment……..………………………………………………..…………………….……………………………………..…Page 3  
Asset Vulnerabilities and threat…………………………………………………………………………….……….……...…Page 3  
Risk owners……………………...…………………………………………………………………………………………..…..…....Page 4  
Impact and likelihood……..……………………………………………………………………………………………….…….…Page 4 Risk acceptance criteria………………..…………….……………………………………………………………………...…...Page 4  
Risk Treatment...…………………………………..……………………………………………………………………………….….Page 5  
Executive Summary…………..…………………………………………………………………………………………………..….Page 5  
References……………………...…………………………………………………………………………………………………...……Page 5

**1.Risk Management Plan:**

**1.1 Purpose,Scope and users:-**

Establishing a Risk Management Plan for DHAEI, a software development company specializing in web registration and hosting and Internet access, is imperative for a variety of reasons. One of the justifications is to ensure the security of the Company’s assets; by developing a risk management strategy, it would be simple to identify and prioritize the threats, enabling immediate action to be taken against the most significant dangers. An additional rationale would be to guarantee business recovery and continuity.

While devising strategies to address incidents will prove beneficial in the long run, the implementation of a risk management plan would guarantee the ability to mitigate potential hazards prior to their impact on the organization's regular operations. The risk management plan would encompass all company employees, given that each individual contributes to the organization's security. Furthermore, the plan's scope would include all organizational operations conducted through its networks.

**2.1 Risk Assessment & Risk Threat Methodology.**

The NIST RMF Framework would serve as the guide for the Risk Assessment procedure. The integration of cyber supply chain risk management, security, and privacy activities into the system development life cycle is facilitated by the Risk Management Framework (RMF). It is imperative to incorporate the perspectives of DHAEI's Chief Information Security Officer **Paul Alexander**, CIO **Amanda Wilson**, and CEO **Alan Hake** into this methodology.

Their ability to enforce stringent regulations pertaining to the adherence to the NIST RMF Framework is facilitated by their leadership positions within the organizations and management of numerous teams.

**2.2 Assets, vulnerabilities, and threats**

**(1)- Outdated Software and Patch Management:**

The company uses Windows Server 2019 and Windows 10. Regularly updating and patching these systems is crucial to address vulnerabilities. The requirement to ensure that all company-issued computers receive approved updates is important for security. However, if this process is not efficiently managed, it could lead to vulnerabilities.

**(2)- VPN Security:**

Remote workers connect using L2TP VPN connections. Ensuring the security of these VPN connections is vital, as VPNs can be targeted by attackers. Multi-factor authentication and regular review of VPN security protocols should be considered.

**(3)- Access Control:**

The security requirement to restrict branch office technicians from having rights to servers outside their respective branches should be strictly enforced. Misconfigurations or overlooking this requirement could result in unauthorized.

**(4)- Multi-Factor Authentication (MFA):**

Enforce multi-factor authentication for remote VPN access. This adds an extra layer of security, even if credentials are compromised.

**2.3 Determining Risk Owners:-**

From the lowest level (Operational Staff) to the middle management IT Managers, section heads, and finally to the senior chief information officer and chief executive officer (CEO), the risk chain of responsibility would progress. At the bottom of the hierarchy, for instance, the IT technicians are assigned with the responsibility of implementing and maintaining security measures. As we move up the chain, the Management is burdened with the responsibility of enforcing security rules and ensuring that their teams are complying with the security protocols. In conclusion, the Senior Management teams, including the **Chief Executive Officer**, would take responsibility for the management efforts and security plans. Their responsibility is to ensure that the organization has a culture that places a strong emphasis on security awareness.

**2.4 Impact and likelihood:-**

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Confidentiality score ( 0 – 10) | Integrity (0-10) | Availability score (0-10) |
| **Outdated Software and Patch Management** | 10 | 10 | 10 |
| **VPN Security** | 10 | 10 | 6 |
| **Access Control:** | 10 | 8 | 9 |
| **MFA** | 10 | 10 | 7 |

**2.5 Risk Acceptance Criteria:-**

During a zero-day attack, the recently implemented security patch poses the largest threat to DHAEI. This is due to the fact that it has a significant impact on the entire CIA Triad. Additionally, the luck of MFA poses the greatest threat and has a high score when it comes to the data protection.

**3.0 Risk treatment:-**

When ranking these hazards, careful consideration should be given to their potential impact on the Company's operations, reputation, and compliance protocols. Urgent attention is required to threats such as illicit data access and vulnerability exploitation, which possess a greater propensity to inflict significant financial or reputational damage. In addition, industry-standard frameworks like the National Institute of Standards and Technology **(NIST)** Cybersecurity Framework can provide guidance for selecting and executing recommended mitigations and responses. This ensures a comprehensive and proactive approach to risk management.

**4.0 Excecutive Summary:-**

After reviewing the DHAEI network, services, hardware, and employee access, recommendations aim to protect critical hardware and data from infiltration. The process starts at the company's main office and involves Domain Controllers, and Files servers. Servers need protection from external threats that could disrupt accessibility, obtain unauthorized access, or install malware, firmware, or ransomware.

Performance, data access, and confidentiality could be compromised, leading to theft or 0 day attack. A firewall required to place and also update the new security patches accordantly to skip and 0 day attack which could cause a huge damage to whole infrastructure CIA trail.

Additional protection includes multi-factor authentication to verify the identity of those accessing services or data.These recommendations are crucial for protecting the privacy, availability, and integrity of our data assets, as well as improving our company's cybersecurity.   
To mitigate cyber dangers, it's important to follow industry standards and execute proactive risk management practices.

**5.0 References-**

1. Patch Management Definition & Best Practices. Rapid7. <https://www.rapid7.com/fundamentals/patch-management/>
2. 10 ways to increase VPN Security. The Front Line Against IT Chaos & Cyber Threats. https://blog.devolutions.net/2021/02/10-ways-to-increase-vpn-security/
3. Making accounts more secure with multi-factor authentication. Microsoft Support. https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661
4. Cybersecurity Framework | NIST. (2024, February 1). NIST. <https://www.nist.gov/cyberframework>
5. Computer Security Division, I. T. L. *About the RMF - NIST risk management framework: CSRC*. CSRC. https://csrc.nist.gov/projects/risk-management/about-rmf