**PART 1.**

Risk assessments are a key part of effective risk management and facilitate decision making at all three tiers of organization level, mission/business process level and information system level.

Threat Sources.

|  |  |  |
| --- | --- | --- |
| **Types of Threat Source** | **Description** | **Characteristics** |
| ADVERSARIAL  Individual (Insider Threat)  Department (Ad hoc)  Company (Vendors, Customers) | Persons, departmental staff and vendors who seek to exploit the company’s network, devices and information systems | The intentions, knowledge of cyber-attacks. |
| ACCIDENTAL  Users (employees)  Administrator | Accidents or errors by employees carrying out their daily activities. | Extent of the threat to devices or the network. |
| STRUCTURAL  Equipment  Power supply  Networking  Operating System | Equipment failure, power outage internet communication failure. | Might be minimal due to backup power supply, data backup. |
| ENVIRONMENTAL  Natural disaster  Fire  Earthquake  Bombing/Terrorism  Infrastructure failure | Disasters that are beyond the control of the company | Severity, duration and impact of the disaster. |

Risk Responses.

Risk Transference involves transferring identified risks to a third party. Buying insurance for example, transfers the risks of financial losses of a negative event to the seller of the insurance.

Risk Avoidance involves taking steps to navigate away from the risk entirely. Not taking on new technologies because of the uncertainty of their success is avoiding risk.

Risk Acceptance involves acknowledging the existence of a risk and choosing to tolerate it without taking any action. It happens in a situation where the cost of mitigating a risk is higher than the potential impact of the risk itself.

Risk Mitigation involves taking measures to reduce the likelihood or impact of a risk. Implementing various security measures to protect against or reduce threats and breaches is mitigating risks.

**PART 2.**

System Security Policy and Risks.

A system security policy starts with identifying potential risks that could threaten the confidentiality, integrity and availability of information systems. This involves managing risks by assessing potential threats to information systems, their vulnerabilities and the potential impact if the risks occur. It continues with regular monitoring and reviews to ensure that the risk management strategies adopted are effective and up to date. The relationship of risk with system security policy concludes with its effective communication with every stakeholder so that roles and responsibilities are understood by everyone involved.

Risk Measurement Evaluation Methodologies. (SANS.org)

* Qualitative Assessment: Uses expert judgment to rate risks based on impact and likelihood with evaluations such as high, medium or low.
* Quantitative Assessment: Assigns numerical values to risks based on financial or operational impact.
* Semi-Quantitative Assessment: it combines the elements of both quantitative and qualitative methods, using a scoring system to rate risks based on some predefined criteria.

Advantages and Disadvantages.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Quantitative Risk Assessment | Qualitative Risk Assessment | Semi-Quantitative Risk Assessment |
| ADVANTAGEs | 1. precise numerical data. 2. Easy comparison of different risks based on their quantified values. 3. Assigns monetary values to risks thereby facilitating cost-benefit analysis. | 1.easier and faster to do. 2. Adaptable to different contexts. 3. Does not require extensive data. | 1.balance between detail and simplicity. 2. Scalable to different levels of complexity. 3. Not as rigorous as quantitative assessment |
| DISADVANTAGEs | 1.complex to perform as it requires specialized knowledge and tools. 2. Greatly relies on the accuracy of data. | 1.subjective and biased. 2. Less precise info, hence insufficient for detailed decision-making. | 1. inconsistency of results due to some level of subjectivity. 2. More complex than qualitative assessment. |

Selecting an Optimal Methodology.

Selecting a risk assessment methodology based on the needs of an organization, advantages and disadvantages involves defining the objectives & scope of risk assessment, evaluating financial & human resources with its timeframe, the assessment methodology to be used considering their advantages and disadvantages. Once the methodology has been determined, conduct a pilot assessment, identify any shortcomings or challenges, adjust as necessary before adoption.

The Four Risk Mitigation Strategies.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Risk Acceptance | Risk Avoidance | Risk Reduction | Risk Transference |
| ADVANTAGEs | 1.cost-free. 2. Resources can be allocated to other critical areas. | 1.completely avoids the potential for loss. 2. Reduces uncertainty by eliminating the risk factor. | 1.potential impact of risks mitigated. 2. Improves the ability to withstand adverse events. | Allow the insured to focus on some other aspect of its business without bothering on risks. |
| DISADVANTAGEs | Exposure to the risk leading to uncertainty and potential financial losses. | 1.potential benefits or opportunities may be missed. 2. Avoiding risks might lead to other challenges. | 1. might be costly because of mitigation measures. 2. Requires continuous monitoring and updates on controls. | 1. limited control over the management of risks by the insurer. 2. Costly due to premiums or fees paid. |

Nesky Aerospace’s Community of Interest is the security team that is responsible for the security and privacy needs of the company. Below is the COI.

**Table 1. Community of Interest**

|  |  |  |
| --- | --- | --- |
| **Name** | **Role(s)** | **Responsibilities** |
| Tomi Talabi | Chief Intelligence Officer | Overseeing the organization’s overall risk management strategy. |
| Nick S. | Digital Technology Director | Integrate cybersecurity into the overall strategy. |
| Aricelli M. | Information Technology Manager | Developing and implementing the company’s information security program and ensures it aligns with business objectives. |
| Phong H. | Information Security Manager | Creates and enforces security policies & procedures, overseeing disaster recovery plan & incident response. |
| Luke G. | Security Auditor | Ensures compliance with regulations & standards, oversees vulnerability and patch management and initiates awareness training as needed. |
| Fulton D. | Security Administrator | Oversee the day-to-day operations of information security and ensure the security of IT infrastructure. |
| Hunter M., Aricelli M., Haley G., Abel O. | Departmental Managers. | Ensure that cybersecurity measures, policies, procedures and standards are implemented within their departments and ensure proper risk management of assets in their departments.  (Akridge, S., 2020.) |

How to approach communicating risk to board of directors, C-level management and stakeholders.

Board of Directors – communicate high level risks that could impact the organization’s strategic objectives by providing quantifiable data to illustrate the potential impact and likelihood of risks using charts, graphs.

C-level Management – detail the activities taken to mitigate risks, the resources needed for the activities, the responsibilities of each resource and how the risk management process is integrated into the overall business strategy and decision-making.

Other Stakeholders – communicating with stakeholders come differently as they have different influences on the business. What each stakeholder needs to know, what they expect and what level of influence must be analyzed before we tailor the information contents to them, how to communicate with them and the appropriate language to use for them. Transparency about risk activities and encouraging feedback from them is essential.

According to NIST RMF, the purpose of risk assessment is to inform organizational risk management processes by determining the potential adverse impacts of the loss of the CIA triad of organizational systems and information.

For the steps to identify the purpose, I will:

* Define the risk management strategy with the purpose of aligning it with the mission and objectives.
* Determine the criticality and sensitivity of the information and systems based on the potential impact of a breach.
* Select the appropriate mitigation controls to the identified risks.
* Implement the mitigation controls.
* Evaluate the effectiveness of the implemented mitigation measures.
* Make an authorized decision.
* Monitor continuously the state of the information system and the management of identified risks.

For the steps to identify the scope, I will:

* Identify the information and assets for risk assessment.
* Categorize the impact levels of the risks to the information and assets to determine appropriate security controls.
* Select the mitigation measures.
* Implement the mitigation measures selected.
* Conduct assessments to ensure that controls are functioning as intended and effective.
* Once the controls are ascertained to be functioning and effective, an authorized decision will be made.
* Continuously monitor the risk assessment measures and regularly update it as needed.

In doing risk assessment, it might be assumed that:

* There is already complete and accurate information about the organization, its systems and potential threats.
* All stakeholders have been identified and will all actively participate in the process.
* Security controls identified and implemented are functioning as intended and applied consistently across all the systems and assets.

The constraints might be:

* Our policies and procedures on the risk assessment process and selecting security controls.
* The laws, regulations and standards we need to adhere to.
* Employees & their level of knowledge, time and budget.
* If we are limited by what infrastructures, we have and lack of current technology.

The sources of information that can be used as inputs are the identified potential threats, possible vulnerabilities, vulnerability scans, past security incidents & breaches, policies & procedures, risk management strategies, network diagrams, feedback from all stakeholders and the Security Operation Center.

**Table 2. Asset Classification.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Information Assets** | **Classification:** Confidential, Private, Public | **Impact on Profitability:** Critical, High, Medium | **Impact on Public Image:** Critical, High, Medium | **Impact on Revenue:** Critical, High, Medium | **Weighted Score / 100** |
| Web Application | Confidential | Critical | Critical | Critical | 92 |
| Servers | Public | Critical | High | Critical | 80 |
| Routers/Switches | Public | Critical | High | Critical | 80 |
| Storage and backup stations. | Private | Critical | Critical | High | 88 |
| Database | Private | High | Critical | Critical | 90 |
| Operating Systems | Private | Critical | Critical | High | 88 |
| Employee information | Confidential | Medium | Critical | Medium | 75 |
| Policy & Procedure manuals | Confidential | Critical | Low | High | 70 |
| R & D documents | Private | Medium | Low | Medium | 65 |
| Contracts and agreements | Private | Critical | Critical | High | 85 |
| Intellectual properties | Confidential | Critical | Critical | Critical | 96 |
| Social Media accounts | Public | Low | Critical | Medium | 68 |

Likelihood of Occurrence Assessment Scale.

|  |  |  |  |
| --- | --- | --- | --- |
| Qualitative | Semi Quantitative |  | Description |
| High | 61 - 100 | 10 | High likelihood of occurrence |
| Medium | 21 - 60 | 5 | Somewhat likely to occur |
| Low | 0 - 20 | 0 | Low likelihood of occurrence |

Impact/Severity if risk occurs Assessment Scale.

|  |  |  |  |
| --- | --- | --- | --- |
| Qualitative | Semi Quantitative |  | Description of Impact |
| High | 61 - 100 | 10 | Critical |
| Medium | 21 - 60 | 5 | Serious or high impact |
| Low | 0 - 20 | 0 | Limited impact. |

**Table 3. Threat Vulnerability Assessment.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat** | **Possible Vulnerabilities** | **Internal or External** | **Probability of Occurrence / Success** | **Reputation Loss if Successful** | **Financial Loss if Successful** |
| DDoS (Distributed Denial of Service) attack | 1. Unpatched systems. 2. Weak passwords. | External | 30% | 30% | 30% |
| Ransomware | 1.Absence of firewall. 2. Non usage of VPN. | External | 20% | 70% | 92% |
| Insider threats | 1.Poor access control measures. 2. Zero analysis on user behavior. 3. Inadequate employee training. | Internal | 25% | 70% | 85% |
| Social Engineering | 1.lack of security training for employees. 2. Lack of user behavior analysis. | External | 85% | 40% | 80% |
| Supply Chain disruptions | 1. Single source of suppliers. 2. Poor communication. | Internal/External | 15% | 85% | 90% |
| Intellectual Property theft | 1.inadequate data encryption. 2. Poor remote access connection. 3. Non-usage of VPN. | External | 10% | 95% | 97% |
| Physical security breach | Inadequate perimeter security. 2. Insufficient physical access control points. 3. Lack of surveillance. | Internal/External | 50% | 10% | 25% |
| Advanced Persistent Threat | 1.Poor incident response process. 2. Lack of IDS/IPS. | External | 40% | 80% | 95% |
| Regulatory non-compliance | 1. Lack of regular audits. 2. Outdated compliance policies. | Internal | 5% | 90% | 85% |
| Equipment failure | 1.Poor maintenance practices. 2. Lack of upgrades in obsolete equipment. | External | 30% | 25% | 75% |
| Access to unauthorized information | 1.Non-usage of principle of least privilege. 2. Wrong usage of access control types. | Internal/External | 20% | 70% | 85% |

**Table 4. Asset Vulnerability Assessment.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** | **Vulnerability** | **Likelihood** | **Impact** | **Risk Rating Factor** |
| Servers | Poor access control, no MFA. | 2 | 4 | 8 |
| Web Application | Absence of firewall, no antivirus. | 2 | 4 | 8 |
| Routers/Switches | No NIDS, lack of DMZ. | 1 | 4 | 4 |
| Storage and backup stations. | No backup plan, poor DRP. | 3 | 5 | 15 |
| Database | No firewall, absence of principle of least privilege. | 2 | 3 | 6 |
| Operating Systems | No upgrade on OS, poor patch management. | 1 | 5 | 5 |
| Employee information | Poor access control, absence of User Behavior Analysis. | 3 | 4 | 12 |
| Policy & Procedure manuals | Excessive permissions, phishing attack, unpatched storage device. | 2 | 5 | 10 |
| R & D documents | No proper file storage, poor physical security, poor data storage. | 3 | 3 | 9 |
| Contracts and agreements | Poor communication, wrong use of language, lack of knowledge. | 2 | 3 | 6 |
| Intellectual properties | Insider threats, non-enforcement of an NDA, weak access control policy. | 3 | 5 | 15 |
| Social Media accounts | Improper use of language, communication gap from senior management, poor Public Relations. | 1 | 5 | 5 |

The risks that are acceptable to Nesky Aerospace are a breach of the router and poor handling of the social media accounts.

If the router is compromised, internal operations will still go on. Communication to the outside world will be affected for the period of compromise. The social media accounts can be done without for a few days. We will communicate with the stakeholders in their preferred way.

The unacceptable risks are intellectual property theft and the breakdown of the storage and backup stations.

References.

NIST SP 800-30 R1, 2012. Guide for Conducting Risk Assessments.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-300r1.pdf>

SANS.org, (n.d.). Cybersecurity Risk Assessment.

<https://www.sans.org/security-resources/glossary-of-terms/cybersecurity-risk-assessment/>