**Name: Vernon Linken**

**ID: 23582206**

**SCW** *Safe Cyber World*

**MASA’s Current Cyber Threats**

**Table of Contents**

**Introduction…………………………………………………………………………………………………………………..1**

**Importance of Risk Assessment……………………………………………………………………………………..1**

**Critical Asset Identification…………………………………………………………………………………………….2**

**Threat Identification………………………………………………………………………………………………………3**

**Threat Assessment…………………………………………………………………………………………………………4**

**References………………………………………………………………………………………………………….6**

**Introduction**

Michigan Aeronautical Science Association commonly known as MASA is a space-based engineering team associated with the university of Michigan. Their focus is on the field of rocketry. They are pioneering in what they do and they have many customers around the word.

As world is stepping up with many different sophisticated technologies, the adversaries who earn living illegally also developed more complex ideas and implementing ground breaking techniques to attain what they desiderate. This report aims to identify some cyber risks which MASA may be facing.

**The Importance of Risk Assessment**

The evolution of the internet technology has evidently brought many benefits to almost all organizations around the world. Unfortunately, not all organizations are aware of the risk of interacting with the cyber word. Cyber risk assessment is one of the critical step in which all organizations should take when interacting with the cyber world. According to CCOHS (2020), Risk Assessment in the context of cyber security is the procedure in which the factors of the likelihood of loss in the organization are identified and precautionary measures are made. By performing a risk assessment in MASA, relevant threats can be found as well as the vulnerable assets. This can help the organization maintain its security policies and procedures in order to prevent loss in the organization.

Adversaries work of exploiting vulnerabilities is systems is ceaseless and incidents can come to pass anytime. Loss of data is what all organizations always avoid. By performing a risk assessment in MASA, the likelihood and the impact of loss in some of MASA’s critical information assets can estimated and prioritized. Australian Cyber Security Centre (2017) has reported that the challenges which they are currently facing include ransomware, social engineering and credential harvesting malware and few more other threats. These threats have no specific targets and can affect the organization as a whole and the individuals. MASA has customers around the word who are interested in space related work and the consequences of not performing a risk assessment in the organization can affect both the organization and its customers due to their consistent unfamiliarity of the cyber threats.

Managing risks is an essential part when it comes to preserving the organization function (Mutune 2020). There are different ways in which the analysis can be beneficial to MASA. Basically, it helps MASA identify their vulnerable assets, allows MASA to comply with government compliances, it mitigates the likelihood of an attack and relevant threats, and it makes the organization aware of the potential attacks (CCOHS, 2020). All the above can help MASA review their security controls and make best decisions based on the risks and current security controls to avoid any loss in the organization. Risks may arise due to weaknesses within an information system. The level of its risk can be define by analysing two main factors (SCU learning resource). These are impact of loss and the likelihood of an attack. Managing these risk may involve different frameworks which suits the risk.

Due to different levels of risks and their nature, different frameworks or approaches are also implement in managing the risk. The framework used in this analysis involves analysing the Likelihood and Consequences Rating in scaling the risks. This approach is known as Qualitative risk assessment. The approach can be more suitable as it uses only five levels of measuring the likelihood which are almost certain, likely, possible, unlikely and rare. This also helps in avoid making estimation errors in other frameworks such as quantitative approach.

**Critical Asset Identification**

The aim of protecting MASA’s information asset is to prevent loss in the organization. Therefore, it is important to identify the most critical information assets in the organization and classify them by their impact of loss in the organization. The questions below will help to identify MASA’s critical information assets.

Questions

1. As a space engineering team, which information asset is the most critical for the success of your projects?

Apart from human resource, there may be some other proprietary information that includes secret procedures, formulas or processes used for managing projects. The loss in these assets may prevent MASA from effectively and successfully managing their projects. Certainly, these information assets should be found in places where technical work takes place. Because MASA’s focus is on rocketry, the most critical asset that can be identified is any **software** created with high-orderly Assembly Language/shuttle (HAL/S) and other programming Language. HAL/S is a real time programming language use by space technologies (Wikipedia, 2020).

1. Which information asset holds the most sensitive and critical data for the organization and is always keep confidential?

As a space agency, keeping information confidential is must. The disclosure of these information can embrace MASA.

Most of MASA’s data is stored using their private **cloud storage** hosted in Sidney office (SCU learning Resource).

1. Apart from MASA’s space facilities, which information asset is the most expensive to replace if loss?

One of the most expensive information asset used by all space agencies is a **satellite**. According to Brown & Harris (2020), the expense of launching a satellite into space may be ranging from $10 million to $400 million. This makes the satellites one the most critical asset in the organization.

1. Space engineering is costly and space agencies often deal with millions to billions amount of money. As a space engineering team which information asset holds most of MASA’s financial information?

Most of the financial records of an organization are stored digitally within **computers** in the financial department?

1. Which information asset involves a lot and most times in processing MASA’s data.

MASA has a 3 other offices in different countries and therefore, there is a need for communication. The mostly used asset to process the information is a **network**. This involves all the components of the network like switches, routers and more other components.

By answering the questions above, the top 5 information assets that are identified are

**Software** (Programs used in for space orbiting vehicles)

**Cloud Storage**

**Satellites**

**Desktops/Laptops**

**Networks**

The next step after the identification of assets is to classify the above assets. The classification of the assets can clarify the criticality and the sensitivity of the asset in the organization.

The method used in classifying these assets is known as weighted factor analysis.

**Risk Management for MASA’s Information Asset**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Information asset** | **Criteria 1**  **Impact on Revenue** | **Criteria: 2**  **Impact on Profitability** | **Criteria: 3**  **Impact on Public Image** | **Weight**  **Score** |
| **Criteria Weight** | 30 | 40 | 30 |  |
| **Software** | 0.5 | 0.1 | 0.1 | 22 |
| **Cloud Storage** | 0.3 | 0.1 | 0.4 | 25 |
| **Satellites** | 1.0 | 1.0 | 1.0 | 100 |
| **Desktops/Laptops** | 0.6 | 0.3 | 0.2 | 38 |
| **Network (LAN)** | 0.8 | 0.8 | 0.8 | 80 |

*To identify the most critical asset in the organization, weight score should be evaluated using the three criteria above. The higher the value of weight, the more critical the asset is. For the above assets, satellite is identified to be the most critical asset in MASA as its weight value is higher.*

**Threat identification**

By going through CISCO, ACSC and other cyber security organization’s threat reports, the top five trending and common threats used by attackers today are:

1. **Ransomware** – a malware which can encrypt data in a computer demanding a ransom to be paid to restore the access. This malicious software can cause a permanent loss in the data.
2. **DNS Hijacking**- This involves compromising the DNS and faking IP addresses. A victim may be redirected to a malicious website that may look legitimate.
3. **Social Engineering** – This involves interacting with human and getting them breaking security policies to gain access to a system. An attack can be successful if CIA is not maintained and other security procedures.
4. **Remote Access Trojan (RATs**)- RAT basically is a software which allows hackers to remotely access a computer which the rat was installed. This software is design in a way that it looks legitimate to the victim. There are various ways in which RAT can be installed in a computer.
5. **Phishing –** phishing is technique used for stealing user’s credentials. This involves sending emails containing log in requests and more other means.

By focusing on MASA’s critical assets, these threats can significantly affect MASA. In order to assess some of the risk which MASA may be facing with its assets, relevant threats and vulnerabilities should be identified, assessed and prioritized. The table below present some threats and vulnerabilities that most suits MASA’s critical assets.

|  |  |  |
| --- | --- | --- |
| **Critical Asset:** | **Relevant threat:** | **Vulnerability/Circumstances:** |
| **Software (used in space orbiting)** | **Human error**  **Remote Access Trojans** | **Weakness in CIA** |
| **Cloud Storage** | **Insider Threats**  **Social Engineering** | **Weak Passwords**  **Lack of Security Architecture in cloud computing**  **Lack of security practices** |
| **Satellites** | **Malicious Software attacks-**  **Remote Access Trojans**  **(hackers can infiltrate computers in ground-stations)** | **High Powered Antennas**  **Lack of security awareness** |
| **Desktop/Laptops**  **(Connected to a networks)** | **Remote Access Trojans,**  **Ransomware** | **Weakness in CIA.**  **Accessing Malicious Websites**  **Malicious emails** |
| **Local Area Network** | **Malicious software attacks** | **Weak firewalls** |

**Threat Assessment**

Most organizations nowadays have websites or blogs created for a specific purpose. Apart from MASA’s five critical assets identified above, their website is the most critical asset of all times.

By analysing the above trending and common threat that most suits a website is DNS hijacking. Hackers can fool anyone who log in to MASA’s website and redirecting them to a malicious site which may look legitimate. However, the most common technique used by adversaries to hack websites is known as cross-site-scripting (xss) (Wikipedia, 2020). Basically, xss allows hackers to modify websites using html and JavaScript (Tech Raj, 2017). Using this technique could obviously affect the Integrity in the CIA as the hacker could possibly modify the website as according to how they desire. MASA’s website contains necessary information and facts about MASA. An unauthorized modification of the website cab embraced MASA and as result can lead to loss in the organization.

Using the qualitative risk matrix (AU&NZ Risk Management Standard 4360), below are MASA’s 6 critical assets and their corresponding risk values.

|  |  |
| --- | --- |
| **Asset:** | **Risk Level:** |
| **Software** | **High** |
| **Satellites** | **Low** |
| **Cloud Storage** | **High** |
| **Network** | **High** |
| **Website** | **Very High** |
| **Desktop/Laptop Computer** | **Very High** |

**References**

Australian Cyber Security Centre (2017), Threat Report,

<https://www.cyber.gov.au>

Brown,G & Harris, W (2020), Remote Sensing Of Environment

<https://www.howscience.howstuffswork.com>

CCOHS, Hazard ID, Risk Assessment, viewed 23 August 2020,

<https://www.ccohs.com>

CISCO, (2019), Threats of the Year, viewed 23 August 2020;

<https://www.cisco.com>

MASA, Taking Michigan to Space, viewed 23 August 2020;

[www.massa.engin.umich.edu](http://www.massa.engin.umich.edu).

Mutune, G, The essential Cybersecurity Controls, viewed 23 August 2020,

<https://www.cyberexpert.com>

SCU Learning Resources

Tech Raj, Cross-Site-Scripting, viewed 2020, 23 August,

<https://www.youtube.com/watch?v=eymxlggL9EQ&feature=share>

Wikipedia, High Orderly Assembly Language, viewed 23 August, 2020,

<https://www.wikipedia.com>