|  |
| --- |
|  |
| INFORMATION SECURITY ASSIGNMENT 2 |
| RISK ANALYSIS AND DATA CLASSIFICATION |

Family Name: David Selvam

Given Name: Visahl Samson

Student Number: 10498743

Unit code and Title: CSI2102 Information Security

Name of Lecturer: Lee Han John

Campus: PSB Academy, Singapore

Course: Bachelors of Science in Cyber Security (FT)

Due Date: 22nd July 2019

Contents

[Introduction 3](#_Toc14591815)

[Executive summary 3](#_Toc14591816)

[Information assets 3](#_Toc14591817)

[Threats associated to the information assets 4](#_Toc14591818)

[Risk model (Weighted Factor Analysis) 5](#_Toc14591819)

[Risk Matrix 6](#_Toc14591820)

[Recommendations/ Countermeasures 8](#_Toc14591821)

[Information classification schema 10](#_Toc14591822)

[References 12](#_Toc14591823)

# Introduction

In information security risk assessment plays a vital role. Generally, risk assessment is a process of identifying the threats that cause potential harm to an organization. In today’s technology all kind the organizations rely on information that benefits them. In order to protect the information it is necessary for the organizations to make proper risk assessment plan. The main purpose of this report is to design a risk analysis and data classification for the dance club named All Stars Dance to protect their CIA triad. The risk analysis is performed mainly to ensure the dance club member’s data is safe. This report contains the identification and classification of information assets, weighted factor analysis, impacts of threats and vulnerabilities & risk rating and countermeasures for the threats identified.

# Executive summary

This risk assessment for Allstars Dance club starts with identification of information assets then moving towards the threats associated with the assets classified, then continues to weighted factor analysis then moves to risk matrix and explaining the recommendations and ends with information classification schema with recommendations.

# Information assets

Information assets of an organization include everything from devices to people that benefits and organization financially. Here in All Dance group the primary information assets are,

* Member details database (include their sensitive personal information)
  + Dance club member number
  + Full name
  + Date of birth
  + Address
  + Phone numbers
  + Test levels (system admins only)
  + Gender
  + Guardian / Parent full name
  + Admin notes
* CMS (Content Management System of their Website)
  + Joomla CMS
  + CMS database
* Payment Gateway
  + SecurePay
  + Payment Database
* Computer systems
  + Desktops/laptops
  + Portable devices
* Email service
  + Mailchimp
* People
  + System administrator
  + Staff
  + Secretary
  + Event Manager
  + Test convertor

# Threats associated to the information assets

The primary threats that are associated with the identified information assets are follow,

|  |  |
| --- | --- |
| **Threat** | **Action by threat** |
| Human | **Intentional**   * Theft * Hacking techniques – shoulder sniffing, network sniffing, exploiting * Personal motivation * Unauthorised access to the system/information   **Unintentional**   * Carelessness * Lack of security knowledge and practices |
| Software | **CMS system**   * Outdated software * Outdated/vulnerable plugins * Technical error that causes process failure |
| Employees | **Admin/staff**   * System misuse/sabotage * Illegal processing of data * Inside the fence activities |
| Forces of Nature | Natural Disasters like Fire, earthquake |

# Risk model (Weighted Factor Analysis)

|  |  |  |
| --- | --- | --- |
| **Weigh factor** | **Meaning** | **Description** |
| 1.0 | High | Threat is highly severe, controls in place is unsuccessful |
| 0.5 | Medium | Threat is capable of causing issues but the controls in place can stop the threat to cause issue |
| 0.1 | Low | Threat is not capable of causing issue also controls in place is successful |

# Risk Matrix

Risk matrix is a tradition and standard method that is used in risk assessment plan. The primary purpose of this risk matrix is to classify the risks depend upon their probability to happen. Based on the severity the impact will be highlighted in different colours.

The impact is calculated based on the multiplication value of consequences and likelihood of the risk to be happen.

|  |  |  |
| --- | --- | --- |
| **Impact** | **Score** | **Definition** |
| High | 100 | The failure CIA is expected and that would cause extremely severe effect on organization. (Gordon and Malik, 2014) |
| Medium | 50 | The failure of CIA is expected to cause serious effect on organization. (Gordon and Malik, 2014) |
| Low | 10 | The failure of CIA expected to cause limited but not serious effect on organization. (Gordon and Malik, 2014) |

The risk score is the result of risk matrix this score is calculated using the formula Consequences X Likelihood

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Consequences | | | Low Impact | Medium Impact | High Impact |
| Likelihood | High | 1.0 | 10 | 50 | 100 |
| Medium | 0.5 | 5 | 25 | 50 |
| Low | 0.1 | 1 | 5 | 10 |

Low Impact Medium Impact High Impact

# Risk Rating

The risk assessment for the given scenario is given below. This assessment contains possible vulnerabilities, likelihood of occurring along with the impact if that occurs, and ends with risk rating.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Examination** | **Vulnerability/Threat** | **Likelihood** | **Impact** | **Rating** | **Colour code** |
| Website | Vulnerable plugins, DOS, unethical usage | Medium | Medium | 50 |  |
| Data Base | Inside the fence,  Misuse | Medium | High | 50 |  |
| Email | Third party handling security practices, unethical usage by employees | Low | Low | 10 |  |
| Information management | Employees, illegal usage of information, former employees | High | High | 100 |  |
| Physical devices (Portable devices) | Theft, Sabotage, Inside the fence | Medium | Medium | 25 |  |
| Payment Gateway | Third Party security practices | Low | Low | 10 |  |
| Management Passwords | Phishing, Sniffing, Key loggers | Medium | High | 50 |  |
| Computer systems/ Network | DOS, DDOS, inside the fence | Medium | High | 50 |  |
| Forces of Nature | Natural Disasters | Medium | Low | 05 |  |
| People | Inside the fence | Low | High | 10 |  |

# Recommendations/ Countermeasures

Each identified threat required unique countermeasure to avoid. The advisable recommendations for the identified threats are following,

**Website**

The All stars dance club’s website hosted in Joomla, it is advisable to follow strong passwords (which contains numbers, letters, symbols), maintaining strong and periodic backups and updates, effective site security monitoring are the recommendations (Docs.joomla.org, 2015).

**Database**

To protect the database it’s advisable to maintain access control and user privileges to fix authorised users to access the database. Encrypting the database information is suggested along with maintenance of regular backup.

**Email**

Educating employees about basic security such as Phishing and workforce ethical practices and usage of dedicated email protection services such as Cisco cloud email is recommended.

**Information Management**

Educating employees about workplace ethics. Revoking all the privileges and accesses from outgoing and former employees while leaving organization.

**Physical devices**

Setting up secure locks, fencing, dedicated access control (bio-metric). Dedicated monitoring using surveillance cameras, sensors to notify in case of unauthorised access to resources (Margaret, 2016).

Also, for portable devices it’s suggested to ensure that all the permissions that are allocated to the staff in their portable devices are revoked/removed as soon they left their job. In this way the AllStars dance club can protect their information from their former staff. Also, regular updates on portable devices are suggested.

**Payment Gateway**

Since, it is handled by third part and the risk of occurrence is low it’s suggested to know about their security/service policies.

**Management Password**

Using a secure password (which contains numbers, letters, and symbols) along with 2 factor authentication is recommended. 2 factor authentications is a feature that can add additional layer of security to an account. In this method the users need to provide their password along with their OTP/ authentication code received via SMS or Email (Rosenblatt & Jason, 2015). Also, using unique password for each systems/account is advisable.

**Computer system/network**

Usage of dedicated IDS, IPS to prevent network security. Placing honey pots into the network. Segmenting the network using VLAN technique (Randy, 2016), effective network monitoring are the recommended method to keep the network/system safe.

**Forces of Nature**

Since, it’s not possible to stop natural disaster it’s recommended to keep regular backup either in another location (offsite) or in Cloud. For All stars dance club it’s recommended to keep their backup using cloud service. So, in this way even if the natural disaster causes any physical destruction they can overcome with the data stored in cloud.

**People**

For People it’s recommended to educate with basic security practices and work ethics. Here in AllStars dance club the secretary has access to all the systems so if insider threat happens it will affect the business heavily.

# Information classification schema

Information classification schema is a process of classifying the information to make sure required security measures are applied to ensure the security of the information. Information classification mostly based on the confidentiality. The four major levels includes in this classification are confidential, Internal, Public and restricted (Irwin, 2019).

**Information classification for AllStars Dance club**

**Confidential**

Database is a vital element everywhere. The data stored in the database is sensitive thus it required high level of confidential. Unauthorised access to the database will cause high impact on organization. Also, it will cause serious issues on CIA triad.

**Internal**

Internal refers to the scheme that consists the actions related to internal usage. Here in AllStars dance club the main actions are information management where it mainly involves transmission of information using computer networks and storing the information. Failure in this level causes loss of integrity.

**Restricted**

Direct access to the systems, unauthorised usage of network of AllStars dance club leads to compromise of confidentiality. For this reason these are considered as restricted.

**Public**

Since, to join AllStars dance club the members are required to register through their website and all the events will be updated into their website for business purposes and since their email will send from parents the website and email categorised under Public. Though there is possibility of information leakage is possible it can be avoided by effective administration.

**Recommendations**

|  |  |
| --- | --- |
| **Confidential** | As mentioned earlier database is vital in business. So, periodic backups, access privileges, continuous monitoring and encrypting the data in database are the recommendations. Also, using database firewall, web application firewall can be considered along with keeping database backup in encrypted format (Nordic, 2018). |
| **Internal** | Since internal communications and information sharing are necessary it’s recommended to use IDS, IPS to monitor the email and activities of employees. Also, Periodic audit on internal policies (primary functions of members) is advisable. |
| **Restricted** | Physical devices require high level security to make sure the data is safe. Using CCTV and threat detection sensors along with proper monitoring are recommended to make sure there is no unauthorised access to the systems. |
| **Public** | Since, public resources are obvious for business website and email are categorised in public. Also, it’s recommended to administrator to authorise before posting anything in website to ensure it don’t cause negative impact on business. Using strong and secure passwords, restricting email attachment size are recommended along with proper security awareness training (Kevin, 2019). |

# Conclusion

In current world information security plays a vital role. So, it’s always better to ensure that the information is secure from both internal and external threats. So, by performing periodic risk assessments will helps the organizations to keep their information safe and gives more insight about the security.

# References

Gordon, A., & Malik, J. (2014). Official (ISC)2® guide to the CISSP® CBK® (2nd ed., pp. 435-437). New York: CRC Press.

Security Checklist/Site Administration - Joomla! Documentation. (2015). Retrieved from <https://docs.joomla.org/Special:MyLanguage/Security_Checklist/Site_Administration>

Margaret, R. (2016). What is physical security? - Definition from WhatIs.com. Retrieved from <https://searchsecurity.techtarget.com/definition/physical-security>

Rosenblatt, S., & Jason, C. (2015). Two-factor authentication: What you need to know (FAQ). Retrieved from <https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/>

Randy, D. (2016). 3 Network Security Architecture Best Practices | Symmetry. Retrieved from <https://symmetrycorp.com/blog/3-network-security-architecture-best-practices/>

Irwin, L. (2019). What is information classification and how is it relevant to ISO 27001? - IT Governance Blog. Retrieved from <https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001>

Nordic, B. (2018). 7 Gold Standard Database Security Best Practices | Secure Cloud Backup Software | Nordic Backup. Retrieved 21 July 2019, from <https://nordic-backup.com/blog/7-database-security-best-practices/>

Kevin, T. (2019). Implementing the top 6 email security best practices for employees. Retrieved 21 July 2019, from <https://searchsecurity.techtarget.com/tip/Implementing-the-top-6-email-security-best-practices-for-employees>