Assignment 1

Deadline: Day 14/10/2017 @ 23:59

**[Total Mark for this Assignment is 20]**

***IT Security and Policies***

***IT409***

**Instructions:**

* This Assignment must be submitted on Blackboard via the allocated folder.
* Email submission will not be accepted.
* You are advised to make your work clear and well-presented, marks may be reduced for poor presentation.
* You MUST show all your work.
* Late submission will result in ZERO marks being awarded.
* Answer the assignment by using your own words otherwise will result ZERO marks.
* Convert this Assignment to PDF just before submission.

Student Details:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Name:**MOHAMMAD HAZAZI  **CRN:**10427 | | **ID:**120003904 |
|  |  |  |

# Policy lifecycle

***Marks 4***

Q1- Explain Information Security Policy Lifecycle with neat diagram and list the responsibilities associated with the policy lifecycle process are distributed throughout an organization in a table.

The Information Security Policy Lifecycle (ISP-LC), is the method taken by the organization before writing any security policy, to ensure that they have an effective, complete, efficient and applicable security policies supported by all users. The ISP-LC consist of several main processes as below :



**Information Security Policy Lifecycle Responsibilities** ( explanation on next table below )

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Position | Board of Directors and/or  Executive Management | Operation  Management | Compliance  officer | Auditor |
| **Develop** | Approve policy in addition to communicate and support the policy. | Policy planning, researching, writing, vetting, reviewing | Policy planning, researching, contributing, reviewing | Monitor policy compliance |
| **Publish** | Take the lead in demonstrating the policy via practice it, engorge it , and educate it to others. | Policy communication to others .  Make it available to others.  Raise the awareness about policy | Policy communication to others .  Make it available to others.  Raise the awareness about policy | Monitor policy compliance |
| **Adopt** | Policy and its implementation becoming a behavior for everyone. | Policy implementation, evaluation, monitoring, enforcement | Policy evaluation | Monitor policy compliance |
| **Review** | Reapprove policy or remove the old ones. | Feedback about policy,  provide recommendation | Feedback about policy,  Provide recommendation | Monitor policy compliance |

|  |  |
| --- | --- |
| Develop | * Identify the need to the policy (what is the reason behind this policy?) * Outline legal, regulatory and operational requirements to aligned the policy with them. * Identify your audience (write in proper language and style). * Assess the policy with expert, IT SME, legal council and regulator. * Review the policy with all impacted entities before authorizing the policy. * Get the final authorization from the executive management or equivalent. |
| **Publish** | * Announce the policy through the management by telling everyone how impotent is this policy for the organization. * Have the new policy available to people whom intended to. In case anyone would like to read and know more about it. * Raise the awareness of the people about the released policy. Through (eLearning, training, presentation, feedback) to reinforce the importance of the policy. |
| **Adopt** | * ensure that everyone understands the policy and how to be implemented. * Monitor the policy compliance and ensure form its implementation (audit, survey, interview, violation & incident report). * Keep the momentum by reinforcing the policy regularly. |
| **Review** | * Review the policy every year, and take the feedback from internal and external, to have the policy keeping up with any changes in the organization or its infrastructure. * Outdated policy should be updated to meet any changes within the organization or its infrastructure. If policy can’t be updated, then it should be removed. |

# Composition of policy documents

***Marks 4***

Q2- a) Explain why standards enable the policy by defining action.

Policies reflect the guiding principles for any organization. Policy by itself is nothing rather than a plain statement for what organization is looking to implement. And, to ensure the effective implementation of a policy, we need to set the standards which will enable the policy by defining the specific actions or minimum requirements to be taken in order to meet the policy compliance. The actions driven from the standards are (Guidelines, procedures, and baselines).

b) Provide an example to show the difference between password policy and password standard.

**Policy,** represents expectations that are not necessarily subject to changes.

**Standard**, is very specific to the infrastructure

|  |  |
| --- | --- |
| Password policy | Password standard |
| 1. All users must have a distinctive user ID and password that comply with the company password standard.  2. Users must not share their password to anyone.  3. If a password was stolen, it must be changed immediately to | 1. All password must be complex including alphanumeric and special characters and not shorter than (10) characters. 2. Passwords must be changed every 90 days. 3. Passwords must not include repeating characters. |

# CIA security model

***Marks 6***

Q3- a) Define the CIA security model.

1. CIA security model, represent the aspects of an information security program. CIA stand for (Confidentiality, Integrity, Availability). Each aspect considered as a major objective of information security.

* **Confidentiality:** only the authorized people who need to see that data can see it and work with it. And then those who are not authorized to see or touch or be aware of that data they can’t see it and work with it.
* **Integrity:** ensure that our data has not been manipulated intentionally or accidentally by unauthorized party.
* **Availability:** we make sure that the authorized people who need to see that data can get to that data when they need it.

b) Provide your own example to describe violation of integrity, confidentiality and availability.

**Confidentiality violation example:**

Security company has taken a project with government, and they have signed Confidentiality Agreement. Part of their job was to conduct an assessment for IT security infrastructure and its weakness. upon finishing the project, the security company start revealing some of security assessment result in that project and use them as case explanation to other company.

This is clear violation as the security company disclose Confidential information, which is against the Confidentiality Agreement they have signed.

**Integrity violation example:**

Someone modify the content of a report your made, and submitted to your manager like it was coming from you.

This is clear violation as the content of the report doesn’t match what you have submitted originally.

**Availability violation example:**

A web developer relay on ISP company to provide his service to his customer, however, the ISP company usually face an interruption to the service, and they don’t have any failover backup link.

This is clear violation to Availability of the service and customer can’t get the service when he need it.

c) What is the difference between data integrity and system integrity.

**Data integrity**

Ensure that information and data changed only in an authorized way.

**System integrity**

Ensure that any system does its job without being affected by any changes from internal or external environment.

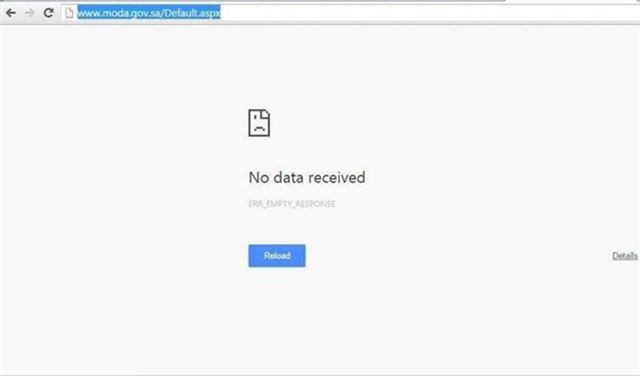
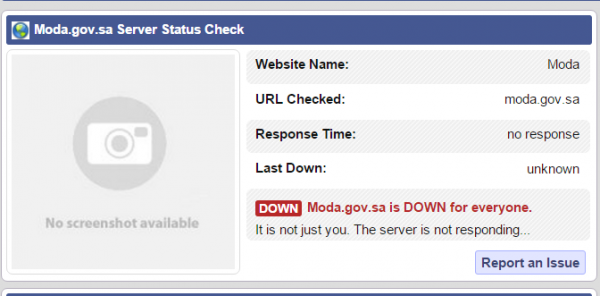
# Understanding hacktivism or DDoS

***Marks 6***

Q4- a) Find a recent article in the internet relating to either hacktivism or distributed denial of service (DDoS) attack.

1. Summarize the attack with your own words.

On 2016 , the Saudi ministry of defense website has received DDos attack from unknown hacker result into forcing the website to stay offline more than 24 hours.

*The website service status checker shows the Saudi Ministry of Defense website is down, by www.hackread.com*

As per the Iranian news agency (Faris), the motive behind the attack was an act of protest against the retribution of Shiite cleric Sheikh Nimr Baqir al-Nimr , who was found guilty due to his involvement in alleged anti-government activities.

1. Explain why the attacker was successful (or not).

The attack was successful due to flooding the website with annoying traffic from multiple computers which lead to network failure as result website become down.

The attack comes from computers usually refer to (botnets), which are effected computers by malicious software through emails or attachment. Once computer is affected it will be connected to the hacker command center, in which he will direct those infected computers to attack like zombies. However, it’s not necessary to make such attack through punch of infected computers. In fact , nowadays you can rent DDoS service to have some taken down.