Assignment 4 - Information Security

Task 1

- individual summary

Author: Sarpreet Singh Buttar
Supervisor: Ola Flygt
Semester: Spring 2016
Subject: Computer Security

Introduction

Information security has become an essential part of every business. Information is considered one of the important assets of every business or company. It is very important to implement information security in a secure and efficient way. For implementing information security, one must have a good knowledge of policies, set of controls, hardware as well as software functions etc. In this task, I am going to give a brief summary of three controls which I will be responsible for in this assignment.

Controls

1 Information Security Incident Management

It is divided in two parts:

1.1 Reporting information security events and weaknesses

The *objective* is to make sure that information security events and weaknesses related to information systems are communicated in a way that makes timely corrective action possible. Procedures for reporting events should exist. All who are involved should be informed of these procedures and be obliged to report as soon as possible.
There should be *an incident response* and escalation procedure about what actions should be taken if a report is made. A point of contact for reporting should be established and well-known as well as available.
Within the *reporting procedures* it should be included that those who made reports should be notified of the results, how to act in case of an information security event and processes of how to deal with any party that commit security breaches. A *duress alarm* may be provided in high-risk environments.
Information security events and incidents may be loss of service, system malfunctions, human errors and so on. They can be used in training for *user awareness* for response to, and prevention of future problems.
Employees, contractors and third party users should report problems immediately, not attempt to solve them, and reporting should be easy and accessible.

1.2 Management of information security incidents and improvements

The *objective* is to ensure that a permanent, effective approach is used in management information security incidents.
For *detecting information security incidents*, there should be a monitoring of systems in place. Incidents and causes of incidents must be identified, and corrective action planned, if necessary. Only authorised personnel can access live systems and data.
From evaluations there might be indications of need for additional controls to limit future incidents. If follow-up on incidents becomes *legal action*, evidence should be collected according to the relevant jurisdiction(s). For *collecting evidence*, internal procedures should be developed and followed.

2 Business continuity management

It is divided in one part:

2.1 Information security aspects of business continuity management

The *objective* is to counteract interruptions to business activities and ensure their continuing. Consequences of failures and disasters should be analysed and information security should be an essential part of the business. Management will include controls for identifying and reducing risks and for limiting the damage of incidents. Events that may cause disturbance must be identified.
Continuity plans which contains information about vulnerabilities of the organisation must be protected properly. Crisis management might be different from business continuity management. The continuity plans should be tried out for possible updates to make sure that they are efficient[1].

3 Compliance

It is divided in three parts:

3.1 Compliance with legal requirements

The *objective* is to avoid breaches of laws and security requirements. Specific legal requirements should be taken from legal advisers, and these may differ from country to country. Statutory requirements are to be defined, documented and updated. Intellectual property rights include software or document copyright, trademarks, patents and source code licenses.
Important *records* should be protected according to statutory, regulatory, contractual, and business requirements. Some records might need to be reserved to meet regulatory requirements and support business activities. The time period and data content for information retention can be according to national law.
Data protection and privacy should be guaranteed according to legislation and possible contractual clauses. Some countries have introduced legislation controlling the collection, processing and transmission of personal data.
Users should not use *information processing facilities* for unauthorised purposes. An organisations information processing facilities of an organisation are intended primarily or exclusively for business purposes. The legality of monitoring the usage varies from country to country.
Cryptographic controls should be used according to relevant agreements and laws. It is recommended to take legal advice before moving the cryptographic controls to another country in order to deal with national law and regulations.

[1] I want to know some more objetive information about this control. All the sub sections in this control are quite relavent to each other, for that reason summary is short. However, I have not add implemenation process, only read it.

3.2 Compliance with security policies and standards and technical compliance

The *objective* is to make sure that everybody is following the organization policies and standards.
Regular reviewing should be carried out in each area by the managers in order to reach the desirable compliance which meets with the security policies and standards. In case of any disobedience, managers should take the necessary actions to detect and evaluate the cause and prevent it from future occurence.
For *technical checking*, expertise are required to find out if the controls (hardware and software) are implemented correctly. These expertise will also help to check the vulnerabilities and capability of controls for handling any illegal access. These types of test usually show us the strength of the system at different states.

3.3 Information systems audit considerations

The *objective* is to decrease the interferance from the information systems audit process in order to increase the effectivenss of it. In addition, protection is necessary to keep the itegrity and audit tools safe.
A well *plan* is required which includes audit conditions, movements and testing of opearational system to decrease the danger on business development growth. It is very important that management must agree with the audit requirements.
The passage to information security tools must be protected to avoid any type of incident. For instance, there is a risk of misuse of audit tools if any unauthorized person access to them. It is very important to restrict *physical access* to reduce the risk. If third parties are elaborated in an audit, high risk tasks such as changing password might need extra protection.

Questions

I think all of three controls which I mentioned above, I do not have any questions related to them. I will still appreciate your feedback if I have not cover any part of the control. However, I have question related to company info document. I read the implementation process of these controls and not sure how to implement them in the fake company scenario. Following are some question related to them.

1) In the company info document, it has been written that each employee will sign an agreement with the company before starting, I want to know that which condition will be in the secrecy paper? I mean, in one of my control it is mentioned that if they (employees) will not follow the organization laws or policies strict actions must be taken against them.

2) It is mentioned that server have no direct protection against physical access, this is against my control. How will I deal with this?

3) The employees PCs have full admin controls, this also does not completely match with the requirement of my controls?