Study topic IT security management assessment 2

What information security is and is purpose

Information security (infosec) can be identified in the effort to protect information assets that represents a value for the company in such way that Confidentiality Integrity and availability (CIA) are preserved and regulated. In fact, information security can be defined as the CIA protection of information assets. The purpose of Information security is to protect the information whether in storage, processing or transmission via policies enforcement, Training and awareness, and technology. The McCumbers Cube gives as an idea of the three main aspect of infosec: information characteristics (confidentiality, integrity, and availability of an information), information location (storage, processing, transmission) and security controls(policy, education, and technology).

Threats, threat actors and threat intelligence

It is crucial for the information security management team to know the threats and vulnerabilities in order to prevent risks against the assets that needs to be protected. The term threat means potential risk whereas threat event means attack that can result in assets disruption. However, threat agents can damage or rob information asset often by taking an advantage of the system vulnerability. The threats are divided in 12 distinctive categories for each category there are different type o threats event that can occur. For example, theft is often associated with illegal confiscation of equipment or information. Theft in particular is associated with other threat category and can occur via espionage or software attack. Threat intelligence is the analysis of the information gathered from existing threats and it can be used to prevent or mitigate threats.

Contingency planning, why would you use it and the type of planning

The contingency plan is part of infosec and aims to protect information during and after unexpected threat event that can occur in a way that is impossible to predict. For example, in case of fire, earthquake or other natural disasters. The contingency plan which is a component of the risk assessment can be used for continuing the operation during and after a threat event or to recover lost assets after an attack. The contingency plan includes:

Incident response

Disaster recovery

Business continuity plan

Preparatory business impact analysis

The business impact analysis is usually discussed in the risk assessment where the risk assessment team is able to point out the business functions and information that are crucial for the enterprise, and then prioritise them in order to protect the company most important assets. Whereas The Incident response is to have a plan for an immediate response to an incident in order to mitigate the impact of adverse events. The Disaster recovery is a written plan that is focus on recovering data or simply restoring functionality on the system. However, for continuing the operation during the accident a company can relay on the business continuity plan.

Governance and role governance plays in the protection of information assets

The governance in infosec is responsible for setting framework that is aimed to protect information within a business and the strategic plans in which the information are secured. Furthermore, they set the vision of the company and can effectively have an impact on how the business is organised. For example, the Industry Framework for Information Security Governance includes some points of security that can be applied on many businesses to secure the information such as conducting annual information security evaluations and risk assessment, implementing policy and procedure based on both risk assessment and security evaluation just to name a few. Additionally, the Industry Framework for Information Security Governance, includes the IDEAL model, which is focus on setting security goals, improvement, and plan integrity. These frameworks can by applied on a broad variety of companies as they commonly point out general policies, procedures, and best practice to achieve cyber security.

Policy and the types thereof, that need to be considered to protect information assets

There are policies that are commonly used to ensure the security of the information. For example, Access control policy that can includes user access guideline to prevent threats or the remote access policy which define permission and procedures that define the conditions in which the system can be accessed remotely. Other policy that are important can be the Business continuity plan that defines the parameter in which the company will operate during an ongoing threats event and the disaster recovery plan that defines the procedures to recover after an incident.

Understand factors that are likely to shift in a organization’s information security

In my opinion the factors that can shift a company’s information security are Lack of policies, procedures, and best practice, followed by the lack of training. In saying that, is highly recommended to enforce security framework in order to have a clear pathway for goals and improvements in term of security. Additionally, the framework adopted should provide with plans that includes training programs to be conducted frequently as the majority of the threat’s events are caused by Human errors.

Approach to security, i.e, a defensive prospect or a offence prospective and how each can benefit a organization security posture.

The cyber security community refers to a defensive prospect when one or more actions are taken in order to prevent, detect and address a vulnerability. Whereas the offence prospective is when ethical hacking is performed to test the system in order to find a solution to potential vulnerable points. These two combined along with policies, procedures, best practice, and training can lead to a more secure system. Moreover, defence prospect and offence prospective are tools that allows the company to find new vulnerabilities and stop potential threats even if the business facing a rapid growth.

Risk management and its components

Risk Management ensure the evaluation of risks and the countermeasures to prevent Threat events. The process undertaken to evaluate risks are risks identification, risk analysis, risk evaluation and risk resolution. For example, the management can use the following tools to evaluate the threats: the weight factor analysis fallowed by risk identification, risk assessment, and risk control.