Information Security Risk Management

Information Security Risk Management

Any organisation’s computer system in the world may have vulnerabilities that have not yet been discovered, even though it is already well protected. This can lead to certain security risks that may cause considerable loss to the organisation.

Information Security Risk Management is to identify and mitigate these potential risks as far as possible, so that the information system’s overall risk level can be lowered.

Risk Analysis

Risk Analysis is a set of risk management tools that includes the following: (1) Asset identification and valuation (2) Threat analysis (3) Analysis of potential risks (4) Recommendations to reduce risks and their impacts. Findings of the analysis will be used to develop the most feasible solution for improvement. As the cost of the best solution is usually higher, the management should strive a balance between cost and benefit.

For typical risk management, there are generally four ways to deal with risks:

(1) Reduce risk

The existing risks of the computer system are minimised without affecting any normal business operation. For example, in order to avoid portable computers from being stolen, they should be locked in cabinets when not in use.

(2) Transfer risk

To shift the risk to another party, either partially or in full. For example, take out insurance for the information system to transfer the risk to the insurance company.

(3) Accept risk

After considering the likelihood of risk and the possible loss induced, it is decided to keep current security measures unchanged and accept the consequences. For example, the risk of data loss for a portable computer containing no sensitive information may be accepted.

(4) Avoid risk

Abort all practices with potential risks to avoid the occurrence of any risks. For example, replace portable computers with desktop computers to avoid any loss by losing a portable computer.

Security Risk Assessment and Audit

Security risk assessment is usually conducted before production of a new information system or on a regular basis after its rollout. The assessment results and recommendations for improvement should be properly documented for review in security audit. Security Audit is a process, in which security review is carried out periodically based on the security policy to make sure that security measures are properly followed.

Security Risk Assessment must be conducted whenever there are major changes in the system or at a pre-determined interval as specified in the security policy.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk