Fundamental Concepts of Data Security
ISEC2001

Business Continuity I

Question 1

Risk analysis is an integral part of the process of developing a security system. What is risk analysis used for and how does it influence the overall security system?

Question 2

An important step in risk analysis is to determine the value of an asset. Give five (5) different questions you think might help with the task of determining the asset value.

Question 3

Give two (2) examples of intangible assets and explain why it is often more difficult to determine the value of an intangible asset than a tangible one.

Question 4

A backup data centre is located in a remote area. It has been determined that in the event of a severe cyclone, which happened twice in the last 40 years, the backup data centre suffers 50% damage. The cost to rebuild the centre is currently $1 million. What is the single loss expectancy for the centre suffering from such a severe cyclone? What is the annualised loss expectancy? If the insurance premium for such events is $10,000 per annum, would it be wise to consider insuring the centre to address the risk? Explain your reasoning.

Question 5

Consider the following risk analysis of a software company

Threat category	Cost per incident	Occurrence frequency
Programmer mistakes	$5,000	1 per week
Loss of intellectual property	$75,000	1 per year
Software piracy	$500	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Theft of information (employee)	$5,000	1 per 6 months
Web defacement	$500	1 per month
Theft of equipment	$5,000	1 per year
Virus, worms, Trojan horses	$1,500	1 per week
Denial-of-service attacks	$2,500	1 per quarter
Earthquake	$250,000	1 per 20 years
Flood	$250,000	1 per 10 years
Fire	$500,000	1 per 10 years

- Calculate the SLE, ARO, and ALE for each threat category listed in the above table.
- How did the software company arrive at the values shown in the table?
- Assume that the company has implemented controls to address the risk shown in the analysis and the new figures after one year are shown below. Assume that the cost per incident figures are still the same. Recalculate SLE, ARO, and ALE values for each category. Comment on the results.

Threat category	Occurrence frequency	Cost of controls	Type of control
Programmer mistakes	1 per month	$20,000	Training
Loss of intellectual property	1 per 2 years	$15,000	Firewall/IDS
Software piracy	1 per month	$30,000	Firewall/IDS
Theft of information (hacker)	1 per 6 months	$15,000	Firewall/IDS
Theft of information (employee)	1 per year	$15,000	Physical security
Web defacement	1 per quarter	$10,000	Firewall
Theft of equipment	1 per 2 years	$15,000	Physical security
Virus, worms, Trojan horses	1 per month	$15,000	Antivirus
Denial-of-service attacks	1 per 6 months	$10,000	Firewall
Earthquake	1 per 20 years	$5,000	Insurance/backup
Flood	1 per 10 years	$10,000	Insurance/backup
Fire	1 per 10 years	$10,000	Insurance/backup

Question 6

A recent security audit at an organisation has revealed that the processor of an important internal server has a critical design flaw that could be exploited to reveal confidential system information. This is a hardware vulnerability and there are no current fixes. It is also determined that it is not cost effective to upgrade to a new server and the current server must continue its operation to serve users within the organisation. The organisation needs to address this particular risk immediately. Identify two (2) strategies that can be used to address the risk. For each strategy, give an example and briefly explain how it helps.

Question 7

List and briefly describe five sections which are usually found in a policy.

Question 8

Describe an example wherein unmanaged changes to IT systems and networks can increase risk to enterprises. Describe how the risk can be minimized if changes are managed carefully.

Question 9

Describe how you would measure the success of a change management program?

Question 10

What are basic elements that you can expect to see in a change management and control policy. Briefly describe each of them.