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?

Risk Management, Risk Assessment and Risk Analysis

Risk Management: Risk management is the overall management to manage risks. Risk Assessment is only part of risk management. Risk management also involves planning and monitoring/maintaining that are not covered in risk assessment.

Risk assessment: is part of risk management and is a framework to manage risk at a particular point in time.

Risk analysis is the actual step carried out to quantify impact, likelihood of different risk items in order to determine the risk levels and for making recommendations.

* Risk analysis is used primarily to identify the threats oto an organisation’s assets and to estimate the potential damage that ma need to be dealt with if any of the threats turned out to be real.
* For example, risk analysis may be used to determine what threats one needs to deal with when protecting a medical database and the cost associated with a case in which some patient records are accessed by unauthorised persons.

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.

Questions:

How much is the cost to acquire

How much is the value of the asset to adversaries

How much is the price others are willing to pay for the assets.

Other questions:

* Cost to acquire or develop the asset
* Cost to maintain and protect the asset
* Value of the asset to owners and users
* Value of the asset to adversaries
* Price others are willing to pay fo the asset
* Cost to replace the asset if lost
* Operational and production activities affected if the asset is unavailablie
* Liability issues if the asset is compromised
* Usefulness and role of the asset in the organisation

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.

Eg. Rep and data

Hard to quantify values of intangible assets which may change over time.

Tangible: eg. computers, harddrive and facilities

Assets may be tangible(computers, facilities, supplies) or intangible (reputation, data, intellectual property). It is usually harder to quantify the values of intangible assets, which may change overtime. How do you put a monetary value on a company’s reputation? This is not always an easy question to answer, but it is important to do so.

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.

SLE = asset value x exposure factor

SLE is the loss that you experience to the asset due to the event, in this case is 1mil, therefore (1mil x 50%) , SLE = 500k

ALE = SLE x ARO

500k x (2/40) = 10k

Since, 10k<25k, lt is wise to pay an insurance premium of $10,000 to cover a potential damage of $25,000 from a cost-benefit perspective.

Other possible answer:

Last 40 years - Twice (Very ambiguous)

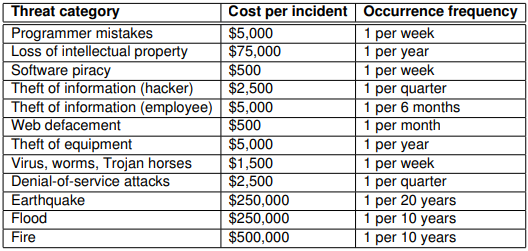
1 year -> (1/40)\*(2) = 0.5% (Exposure Factor)

SLE -> 500k

ALE = 500k x (1/20) = 25k (May be fixed or minimum or maximum)

Question 5

Consider the following risk analysis of a software company

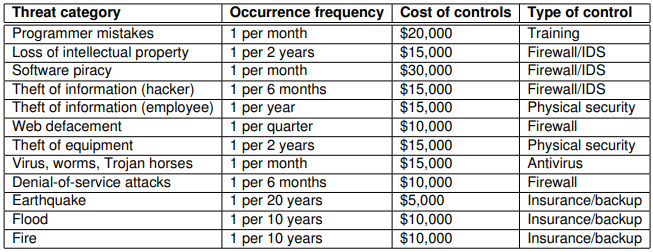


Calculate the SLE, ARO, and ALE for each threat category listed in the above table.

• 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.



SLE = Cost of the Incident x 1 (for all because it only takes into account one incident and the overall frequency for all is 1)

ARO

1. 52 = 1 x 52weeks
2. 1

ALE

1. $260 000= 52 x $5000

If ALE after is the same or more than the ALE before, the control is not effective

Answer:

| Threat Category | Cost/Incident  ($) | Occurence freq. | SLE | ARO | ALE |
| --- | --- | --- | --- | --- | --- |
| Programmer mistakes | 5,000 | 1 per week | 5,000 | 52.0 | 260,000 |
| Loss of intellectual property | 75,000 | 1 per year | 75,000 | 1.0 | 75,000 |
| Software piracy | 500 | 1 per week | 500 | 52.0 | 26,000 |
| Theft of information (hacker) | 2,500 | 1 per quarter | 2,500 | 4.0 | 10,000 |
| Theft of information (employee) | 5,000 | 1 per 6 months | 5,000 | 2.0 | 10,000 |
| Web defacement | 500 | 1 per month | 500 | 12.0 | 6,000 |
| Theft of equipment | 5,000 | 1 per year | 5,000 | 1.0 | 5,000 |
| Virus, worms, Trojan horses | 1,500 | 1 per week | 1,500 | 52.0 | 78,000 |
| Denial-of-service attacks | 2,500 | 1 per quarter | 2,500 | 4.0 | 10,000 |
| Earthquakes | 250,000 | 1 per 20 years | 250,000 | 0.05 | 12,500 |
| Flood | 250,000 | 1 per 10 years | 250,000 | 0.1 | 25,000 |
| Fire | 500,000 | 1 per 10 years | 500,000 | 0.1 | 50,000 |

The company may subjectively evaluate the cost per incident, and may have record of previous incidents to estimate frequency. Estimates from other sources may also be available.

Except for insured items (fully cover the damage), SLE generally does not change even when new controls are put in place, only ARO and ALE change.

| Threat category | SLE | ARO | ALE  (After) | ALE (before) | CC | Y/N |
| --- | --- | --- | --- | --- | --- | --- |
| Programmer mistakes | $5.000 | 12 | $60,000 | $260,000 | $20,000 | Y |
| Loss of intellectual property | $75,000 | 0.5 | $37,500 | $75,000 | $15,000 | Y |
| Software piracy | $500 | 12 | $6,000 | $26,000 | $30,000 | N |
| Theft of information (hacker) | $2,500 | 2 | $5,000 | $10,000 | $15,000 | N |
| Theft of information (employee) | $5,000 | 1 | $5,000 | $10,000 | $15,000 | N |
| Web defacement | $500 | 4 | $2,000 | $6,000 | $10,000 | N |
| Theft of equipment | $5,000 | 0.5 | $2,500 | $5,000 | $15,000 | N |
| Virus, worms, Trojan horses | $1,500 | 12 | $18,000 | $78,000 | $15,000 | Y |
| Denial-of-service attacks | $2,500 | 2 | $5,000 | $10,000 | $10,000 | N |
| Earthquakes | $0 | 0.05 | $0 | $12,500 | $5,000 | Y |
| Flood | $0 | 0.1 | $0 | $25,000 | $10,000 | Y |
| Fire | $0 | 0.1 | $0 | $50,000 | $10,000 | Y |

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.

Transfer risk

Eg. Purchase insurance : Insurance provider pay for the damage if there are damage

Accept the risk

Shld know what will happen assuming the cost of the asset outweighs the risk and the benefits

Mitigate the risk

Put controls on the risk, put

Early detection and response

Create incident response plan to deal with such an attack

Answer:

It is not expected that Prevent or Avoid strategies can be used because of the constraints.

* Strategy 1 : Mitigate the risk. Monitor the server and ask users to monitor their accounts for any suspected activity so early detection and response can be performed. Encrypt user data and perform frequent backup to prevent data from being stolen or damaged. Create incident response plan to deal with such an attack.
* Strategy 2 : Accept the risk. This strategy accepts the risk, knowing that it could happen - assume that the cost much outweighs the benefits.
* Strategy 3: Transfer the risk. This means transfer the risk to another organisation. The simplest form being purchasing insurance. If there is any damage caused by such an attack, the insurance provider will pay the damage.

Question 7

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

Choose four from the following:

* Purpose: Explains the reason for the policy
* Related documents: Lists any documents (or other policy) that affect the contents of this policy
* Cancellation: Identifies any existing policy that is cancelled when this policy becomes effective.
* Background: Provides amplifying information on the need for the policy
* Scope: States the range of coverage for the policy (to whom or what does the policy apply)
* Policy statement: Identifies the actual guiding principles or what is to be done
* Action: Specifies what actions are necessary and when they are to be accomplished
* Responsibility: States who is responsible for what
* Ownership: Identifies who sponsored the policy and from whom it derives its authority, as well as defines who may change the 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.

**Example**

1. Remote access to the internal server - opens the firewall port, introduces unauthorised hackers to also gain access to internal server remotely

**How**

1. Impl change management process whereby approval has to be granted by the superior before the firewall administrator can open the firewall port to allow access to the internal server. Only when he is granted access to open the access to the internal server, the firewall administrator should also monitor traffic from remote to internal server to make sure that the traffic is legitimate and not suspicious.

Question 9

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

Compare the outcomes vs expectations the organisation has ( eg on time, on budget, meats tech and busin or human obj)

Answer

This is an open question: One obvious approach is to compare the delivered outcomes and the expectations before the change.

Some other examples can also include:

* Installation: It is on time
* Installation: It is on budget
* Installation: It meets the technical objective
* Implementation: The business objectives are met
* Implementation: The human objectives are met

Question 10

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

Change Management is the discipline of understanding, adjusting and adapting to a new normal after an enterprise transformation.

Change control is the process of how changes to requirements are sourced, analyzed, managed, and included in the roadmap and implementation schedule.

Change Management is about molding hearts and minds. Change Control is about governing the requirements management.

Change Management is about not letting investment into a transformation come to naught. Change Control is about not letting the requirements runaway train derail a project or a program.

Change Management may or may not involve technology involvement. Change Control is a part of the overall IT enablement realm.

Change Management could impact an entire company. Typically, Change Control is about a specific project and a set of requirements.

Question 11

Using the quantitative risk assessment approach, a software company is assessing the risk due to programmer mistakes which happen five (5) times every four (4) weeks on average and cause a damage of $10,000 per incident.

* Calculate the current SLE, ARO and ALE values.
* The company is considering two possible controls described below to address this risk. Using the cost-benefit analysis (CBA) approach, derive the SLE, ARO, ALE, ACS and CBA values for each case and state clearly which control should be selected to address the risk due to the programmer mistakes.
* Control A (training staff) costs $150,000 per annum and reduces the frequency of mistakes to one (1) every fortnight.
* Control B (smart backup and version control) costs $100,000 per annum and reduces the damage to $5,000 per incident.
* Current values
* SLE = $10,000
* ARO = 52 x 5/4 = 65
* ALE = 65 x $10,000 = $260,000
* Control A
* SLE = $10,000
* ARO = 52 x ½ = 26
* ALE = 26 x $10,000 = $260,000
* ACS = $150,000
* CBA = $650,000 - $260,000 - $150,000 = $240,000
* Control B
* SLE = $5,000
* ARO = 65
* ALE = 65 x $5,000 = $325,000
* ACS = $100,000
* CBA = $650,000 - $325,000 - $100,000 = $225,000
* Conclusion: Control A should be selected because iths CBA is better than that of Control B by $15,000

Question 12

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

Take for example, a team of developers that has just written a much better looking and easier to use version of the organisation’s website. The only problem is that it cant be tested by the remote QA team because the firewall is blocking access. Waiting for change management approval could take weeks, so as the firewall admin, it may be very tempting to want to help out the development team by temporarily opening a port on the firewall. Sadly, we’ve all seen some variation of how that story ends: a worm or Trojan is introduced onto the internal network, a sniffer is planted on a server and credentials are stolen, or a previously protected database is exposed to attackers.

Question 13

Explain the differences between the two roles in a change management process: Change Manager vs Change Coordinator

* Hierarchy: as far as the hierarchy is concerned, Change Manager sits above Change Coordinator, Change Manager actually appoints Change Coordinatior(s). There could be multiple Change Coordinators for multiple business IT units, each looking after their own area. However, usually there is only one Change Manager.
* Responsibilities: Change Manager has the overall responsibility for the organisation and acts at a high level. A Change Coordinator on the other hand is usually appointed for a particular change, and “responsible for planning and coordinating all of the phases of the change from initiation through acceptance and documentation” . Change Coordinators will provide updates to Change Manager on a regular basis. That is to say that Change Coordinators assist Change Manager.