Risk Management: Risk Assessment and Planning

License

You may wish to save a copy of this document that you can modify.

For this specific exercise, you are encouraged to work together on the same document/tables with other (up to 10) students. If you work as a group (and everyone in your group agrees who was involved), you will all receive the same XP rewards.

Scenario

Consider this case:

> You work for an online retailer that has a website, with online shopping. You accept credit card payments, and store details of transactions in a database. You also provide a mailing list for customers.

You can make assumptions about the business that you think are realistic. List the assumptions you have made about the business:

Risk assessment: identification

Given the scenario above, fill in the table below with some potential threats and vulnerabilities that you identify.

- Start by identifying general threats the organisation could face (aim for at least 5)
- For each general threat, list as many process vulnerabilities as you can think of (non-technical weaknesses in procedures)
- For each threat, List technical vulnerabilities that may apply (for example, flaws in the website could allow attackers to access the database)

Table entries created by: ______________

Category of threat	**Process (non technical) vulnerabilities / threats**	**Technical vulnerabilities / threats**
Lose our customers, due to loss/ leakage of information	*Someone tricks a member of staff into giving over someone else's account details*	*Attacker gets all the credit card details via an SQL Injection*

Save a copy of the above table, as evidence that you have completed this part of the task.

Label it or save it as “Risk-1”. Saving a copy of this document is fine.

Risk assessment: magnitude

For 10 specific threats/vulnerabilities (taken from columns 2 and 3 in the table above), determine the magnitude of risk, and enter into the table below:

- Estimate the likelihood for each risk (.5 = 50% chance it would happen in any year)
- Estimate the impact on the business on a scale of 1 to 10
- Estimate the annual cost if the event was to occur (just guess as well as you can)
- Calculate the risk impact

- Calculate the ALE

Table entries created by: _____________

Threat	**Likelihood (0-1)**	**Impact (1-10)**	**Annual cost**	**Risk impact (likelihood * impact)**	**Annual loss expectancy** **(likelihood * annual cost)**
Attacker gets all the credit card details via an SQL Injection	*.10, Unlikely (we are careful, and we use countermeasures)*	*8, this could ruin our reputation*	*£70,000, Could lose lots of business if customers lost trust in us*	*.8 (8/100)*	*£7,000*

Save a copy of the table, as evidence that you have completed this part of the task.

Label it or save it as “Risk-2”.

Planning responses

For each threat or vulnerability identified in the table above (Table 2), list at least two risk solution alternatives.

For each alternative, state whether risk is accepted, avoided, mitigated, shared, or transferred.

Very roughly attempt to guess at total cost of ownership (purchase + yearly operating costs).

For each threat/vulnerability, recommend one solution that you think is best suited, with one sentence justifications.

Threat	**Solution 1**	**Solution 1 TCO**	**Solution 2**	**Solution 2 TCO**	**Solution 1 or 2?**
Attacker gets all the credit card details via an SQL Injection	*Modsecurity* *- risk is mitigated*	*£800*	*PayPal (stop accepting credit cards)* *- risk is avoided*	*£3000*	*Recommend solution 1, PayPal takes a % of sales, modsecurity is much cheaper than ALE of threat.*

Save a copy of the table, as evidence that you have completed this part of the task.

Label it or save it as “Risk-3”.

What to show your tutor for XP rewards:

Show your tutor each of the above (in red) evidences. You (or your group) may be asked to justify your decisions. This will be used to allocate XP for the module. Further details of the XP rewards and requirements are available on the *My XP* site.