University of Oslo
INF3510 Information Security
Autumn 2018
Workshop Questions

Lecture 8: Risk Management and Business Continuity Management

Question 1: Risk factors

A possible definition of information security risk is: *risk = likelihood × impact*

a. Explain what is meant by *likelihood* and *impact* in this definition.
b. Discuss, e.g. with a relevant example, whether this is a reasonable definition.
c. Mention factors that contribute to *likelihood* of a security incident (threat occurrence).
d. Discuss whether it is meaningful to analyse risk based on detailed factors (such as threat agent motivation and capacity) during a practical risk analysis.

Question 2: Risk management decisions

The Risk Management Process specified in ISO 27005 indicates two decision points.

a. Describe a situation where the answer to risk decision point 1 (after the risk assessment) could be negative, thereby requiring a revision of the context establishment and risk assessment phases.
b. Describe a situation where the answer to risk decision point 2 (after the risk treatment plan) could be negative, thereby requiring a possible revision of all the previous risk management phases.

Question 3: Risk description

How should each risk be described?

Question 4: Qualitative risk

a) Assume that a risk assessment uses three levels of likelihood (low, medium, high) and three levels of impact/consequence level (minor, moderate, major). Draw an appropriate table of qualitative risk that uses 5 qualitative risk levels.
b) What is the basis for specifying the qualitative risk levels in the table?
c) How is the table used to determine risk levels?

Question 5: Relative / Semi-quantitative risk

a) Assume a risk assessment method with four relative levels of likelihood: 0 (extremely rare), 1 (rare), 5 (likely), 10 (very likely), and four relative levels of impact/consequence level: 0 (negligible), 1 (minor), 5 (moderate), 10 (major). Draw an appropriate table of relative / semi-quantitative risk that uses 7 numerical relative risk levels.
b) What is the basis for specifying the relative risk levels in the table?
c) How is the table used to determine risk levels?

Question 6: Quantitative risk

Consider a quantitative risk analysis for a business. A specific threat is expected to result in a security incident every two months at a cost of $3 000 per incident.

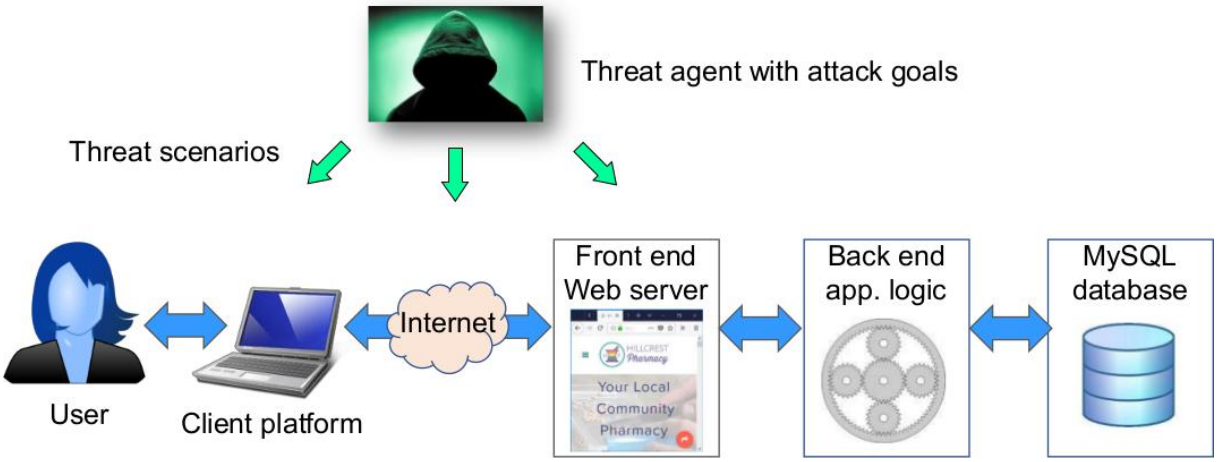
a. Compute the single loss expectancy (SLE) and the annualised loss expectancy (ALE).
b. How should the ALE be used in deciding how to treat this risk?
c. Once controls are put in place, how will they change a later risk analysis?
d. Instead of reducing the risk, name two alternative ways to treat a risk.

Question 7: Qualitative vs. quantitative risk

In what way are qualitative and quantitative risk analysis different? Explain one significant drawback of each type.

Question 8: Threat modelling

Consider the case of an online pharmacy, where the diagram below illustrates the main elements in the e-commerce architecture, as well as abstract threats.



It can e.g. be assumed that the attacker (threat agent) has as goal to 1) get control of user accounts and their purchasing history, 2) steal the user database (and passwords), 3) sabotage, DDoS or deface the website, or 4) store malicious content (XSS, malware, exploits) on the website. You can also consider other attack goals.

a. Describe relevant threat scenarios for each attack goal you want to consider. Don't get stuck by the lack of detail in this case description, you can make any assumption you want. The important thing is to be able to identify and articulate relevant threat scenarios, i.e. steps the attacker must take to reach a specific goal.
b. For each threat scenario, suggest security controls that can block or mitigate the threat.

Question 9: The misnomer: "ROS-analyse"

a. What is the problem with the concept of "Risk and Vulnerability Analysis" typically used in a Norwegian risk management context (ROS-analyse) ?
b. Why is "Threat and Risk Analysis" (TOR-analyse) a better term?

Question 10: Business impact analysis

c. What is special about risks related to disasters, in terms of likelihood and impact ?
d. As part of business continuity planning, a BIA (Business Impact Analysis) is often performed. Briefly explain the purpose of a BIA.
e. Why is BIA often more meaningful than a traditional risk assessment in case of BCM and planning for disaster recovery.

Question 11: Maximum tolerable downtime

a. Specify the typical MTD (Maximum Tolerable Downtime) for a business function that is defined as (i) critical; (ii) non-essential.
b. Assume that the information processing facilities of an organisation has suffered considerable damage, seriously impacting the business functions. How is the MTD taken into account when deciding whether business recovery at an alternative site should be invoked?