University of Oslo
INF3510 Information Security
Spring 2011
Workshop Questions

Lecture 13: Privacy and Regulatory Requirements

QUESTION 1

The Basel II agreement is important for the financial sector.

a. Briefly describe the purpose of Basel II, and when the first version was published.
b. What is needed to make Basel II mandatory for banks?
c. Basel II specifies requirements for both operational risk and credit risk. Mention 3 specific areas of operational risk described by the Basel II agreement that are relevant for information security.

Answer

a. The purpose of Basel II, which was initially published in June 2004, is to create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face.
b. Governments must enact Basel II as law to make it manadoty for banks.
c. Operational risk arreas:
    - Internal Fraud - misappropriation of assets, tax evasion, intentional mismarking of positions, bribery
    - External Fraud- theft of information, hacking damage, third-party theft and forgery
    - Business Disruption & Systems Failures - utility disruptions, software failures, hardware failures

QUESTION 2

There are several laws regulating electronic and digital signatures around the world.

a. What is the relevant EU directive called, and when was it published?
b. What is the goal of the EU directive?
c. What is the corresponding Norwegian law called (in Norwegian or English), and when was it published?
d. Which evaluation assurance level is required of equipment to produce “advanced signatures based on qualified certificates”.

Answer

a. Community framework for electronic signatures, published 13 December 1999.
b. The goal of the directive is to provide a harmonized framework for the provision and use of electronic signatures in Europe.
c. Norwegian: LOV 2001-06-15 nr 81: Lov om elektronisk signatur (e-signaturloven). English: Electronic Signature Act, 2001
d. EAL4+

QUESTION 3

a. When did the OECD issue its guidelines on data privacy protection?
b. When did the EU publish the Data Protection Directive
c. When came the first data privacy act in Norway, and what was its name?
d. When came the current data privacy act in Norway and what is its name?
e. Briefly describe the purpose of the “US-EU Safe Harbour Program”.

Answer

a. In the 1970s the introduction of universal personal numbers in the Scandinavian countries combined with electronic data processing created the possibility of collecting large amounts of information related to individuals, and also the possibility of misusing that information. Sweden took the case to the OECD which issued guidelines on privacy in 1980. Subsequent legislation around the world is based on the OECD guidelines.
b. The EU Data Protection Directive came in 1995.
c. Personregisterloven (Person Register Act) 1978.
d. Personopplysningsloven (Person Information Act) 2001
e. Safe Harbour is a voluntary program that companies can opt into by adhering to the 7 principles of the EU Data Protection Directive. EU countries are allowed to export personal info to companies that adopt the Safe Harbour program.

QUESTION 4

The OECD guidelines specifiy a set of principles for the protection of personal data.
a. Explain the *Security Safeguards Principle*.
b. Explain the *Individual Participation Principle*.

Answer

The principles from the OECD guidelines can be explained as follows:
a. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
b. Individual Participation Principle: An individual should have the right:
    a) to obtain confirmation of whether or not the data controller has data relating to him;
    b) to have data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
    c) to be given reasons if a request made under (a) and (b) is denied, and to be able to challenge such denial; and
    d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

QUESTION 5

In addition to the Data Protection Directive, the EU has issued two more directives that are relevant for privacy.

a. What is the goal of the E-Privacy Directive (Directive 2002/58/EC)
b. What is the goal of the Data Retention Directive (Directive 2006/24/EC)
c. In case of conflict between laws based on the Data Protection Directive and the Data Retention Directive, which will normally carry the most weight, and why?

Answer

The principles from the OECD guidelines can be explained as follows:

a. It deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies.
b. Operators of member states must store citizens' telecommunications data for six to 24 months, so that police and security agencies will be able to request access to details such as IP address and time of use of every email, phone call and text message sent or received. A court order will be needed for requests to access the information.
c. Laws based on the Data Retention Directive will cary more weight because the need to fight crime and terrorism is seen as more important than the need to protect personal information.