University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions

Lecture 2: Security Management, Human Factors in Information Security

Question 1

- Look at the list of standards in the ISO27000 series, e.g. on Wikipedia, http://en.wikipedia.org/wiki/ISO/IEC_27000-series
- Look at the NIST SP800 (special publications) series on: http://csrc.nist.gov/publications/PubsSPs.html

a. Try to find corresponding publications from the ISO 27000 series and from the NIST SP800 series.
b. What are possible drivers for developing IT security standards in general, and for different organisations to develop separate sets of similar standards.

Question 2

a. How are the standards ISO/IEC 27001 and ISO/IEC 27002 related?
b. Which one of the standards can be used for certification, and why?
c. How should an organisation determine which security controls to implement?

Question 3

a. ISO27002 and 20CSC have the same scope. Create a mapping of the correspondence between the 14 security control objectives of ISO27002 and the 20 critical security controls of 20CSC v.6.1. The lecture presentation L02 gives an overview of the controls. You find the detailed control documents on the INF3510 wiki, but you don't really need them here. It can be useful to do this exercise with pen and paper, or using a whiteboard.
b. Make a judgment about how well aligned they are.

Question 4

Assume that Company A and Company B of similar size become victims of cyber attacks, and that as a result both companies suffer heavy damages that negatively affect customers and shareholders. When investigating the events, it was found that Company A had practiced due diligence and due care, whereas Company B had not. Assuming that the damages to both companies were equal, explain the possible differences, if any, in consequences and sanctions against management of the companies.

Question 5

a. Describe ways to use social engineering for;
   1. getting unauthorized access into a company building,
   2. installing malware on the personal computer of the CEO of a company.

   Get inspiration from SANS InfoSec Reading Room on Social Engineering (http://www.sans.org/rr/whitepapers/engineering/), or other relevant sources.
b. Assume that staff are the intrusion-detection function against social engineering attacks. What would be a false positive and a false negative in this scenario?
c. Let us consider a firewall as an analogy for human defense against social engineering attacks. Firewalls must be programmed and configured to provide adequate protection. What would be the analogue process for making sure that staff provide adequate protect against social engineering attacks?