University of Oslo
IN2120 Information Security
Spring 2018
Workshop Questions

Lecture 5: 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. What is the meaning of "System" as the last word in the acronym ISMS?
c. Which one of the standards can be used for certification, and why?
d. 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. The lecture presentation (p.16 and p.18) gives an overview of the control categories. Put e.g. p.16 and p.18 next to each other and draw lines between them
b. Make a judgment about how well aligned the standards ISO 27002 and 20CSC are.

Question 4

The standards *ISO/IEC 27002* and *CIS-20CSC-V7* describe various security controls. Information about the standards can be found on the IN2120 wiki.

a. How can the effectiveness of a specific security control be measured?
b. Below are examples of security controls from *CIS-20CSC-V7*. How can these controls be measured? You can suggest a measurement method, or you can look at the companion document *CIS-Controls-Measures-and-Metrics-V7*.
   i) CIS Control 2.2. Ensure that Software is Supported by the Vendor
   ii) CIS Control 16.9. Disable Dormant Accounts

Question 5

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 implemented an ISMS and had good maturity for information security management, whereas Company B had no ISMS in place and only ad-hoc information security management. 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 6

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 the human defense against social engineering attacks as an analogy to network firewalls. In order to provide adequate protection, firewalls must be correctly programmed and configured. What would be the analogue process for making sure that staff provide adequate protect against social engineering attacks?