University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions

Lecture 2: Security Management, Human Factors & Physical Security

The standards ISO/IEC 27001 and ISO/IEC 27002 are available to UiO students online via the INF3510 wiki pages https://wiki.uio.no/mn/ifi/INF3510-2012/. You need to use your UiO logon to access the wiki pages.

QUESTION 1

Check out the status of the ISO27000 standards series, e.g. on Wikipedia.

a. Which standards have been published?
b. Which standards are planned?
c. Suggest possible drivers for developing new IT security 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

Briefly and clearly explain the PDCA model applied to ISMS processes.
Plan - Do - Check - Act model outlined on page v of ISO/IEC 27001.

QUESTION 4

a. What is a social engineering attack? See e.g Harris p.967, SANS InfoSec Reading Room on Social Engineering (http://www.sans.org/rr/whitepapers/engineering/), or any other relevant source.
b. Describe three typical social engineering attack strategies.
c. Assume that people are the access control function against social engineering attacks. What would be a false positive and a false negative in this scenario?
d. When using a firewall as an analogy for human defense against social engineering attacks, what would then be the analogy of the firewall configuration?

QUESTION 5

Access control mechanisms fall into one of two categories: physical or logical.

a. When is physical access control not enough or not possible?
b. Give three examples of physical access control mechanisms.
c. What is meant by a multilayered approach to physical access control?

QUESTION 6

a. What does the abbreviation CPTED stand for?
b. How does CPTED work?
c. Which are the main principles used in CPTED

QUESTION 7

a. Create a mapping of the correspondence between the 11 security domains of ISO27002 and the 10 security domains of CISSP.
b. Make a judgment about how well aligned they are.
c. Mention security topics that you think are missing in one or the other.