University of Oslo
INF3510 Information Security
Spring 2015
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 developing separate sets of similar standards.

Answer

a. Below are groups of related standards from ISO and from NIST. Many more corresponding standards can be found.

- IS Management
  ISO 27001 — Information security management systems — Requirements
  ISO 27002 — Code of practice for information security management
  ISO 27003 — Information security management system implementation guidance
  ISO 27007 — Guidelines for information security management systems
  SP800-14: Generally Accepted Principles and Practices for Securing IT Systems

- Security measurement
  ISO 27004 — Information security management — Measurement
  SP800-55: Performance Measurement Guide for Information Security

- Security risk management
  ISO 27005 — Information security risk management
  SP800-30: Guide for Conducting Risk Assessments
  SP800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

- Incident management
  ISO 27035 — Security incident management
  SP800-61: Computer Security Incident Handling Guide

b. Drivers behind standards can be:
    - a real need for a new standard,
    - interest/ambition of individuals and organisations to define their own standards
    - The US government does not want to depend on ISO, and the rest of the world does not want to depend on NIST.

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?

Answer

a. ISO/IEC 27001 is a model for setting up and managing an ISMS, i.e. establishing and operating a security program within an organisation. ISO/IEC 27002 is a checklist of security contorols that an organisation should consider implementing.
b. Organisations can only be certified against ISO/IEC 27001 not against ISO/IEC 27002. This is possible because ISO 27001 describes a process for quality control in security management which is more or less the same for all organisations, and can be verified to be in place by an external party. ISO 27002 describes a large number of controls, of which not all are relevant for every organisastion, so it is impossible to verify that the necessary controls are in place in general. However it is of course possible to verify that specific controls are in place, which is typically done by IT auditors.
c. Risk assessment is used to determine where controls are needed. The most appropriate controls are selected to match the risk.

Question 3

a. Create a mapping of the correspondence between the 14 security domains of ISO27002 and the 10 security domains of CISSP.
b. Make a judgment about how well aligned they are.

Answer

BS 7799, which was the original version of ISO 27002, contained 10 categories of security controls. Currently ISO 27002 has 14 categories of security controls. CISSP has always had 10 domains of CBK (Common Body of Knowledge). Some of the sections/domains are more or less the same, but others are specific to either ISO 27002 or to CISSP CBK, so there is no 1-to-1 mapping between the two documents.

Digital forensics and cyber security are relatively new topics. CISSP tends to integrate new topics on one of the 10 domains, whereas ISO 27001 tends to define new categories.

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.

Answer

In general, management of companies is responsible for practicing prudent management, which means that they must practice due dilligence and due care. Management of Company B failed to do that, and could go to prison or be fined as a result, e.g. under the Sarbanes-Oxley act in the US, or the Basel II agreement in Europe.

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 people are the access control function against social engineering attacks. What would be a false positive and a false negative in this scenario?
c. When using a firewall as an analogy for human defense against social engineering attacks, what would be the social engineering analogy of configuring the firewall tp protect against network attacks?

Answer

a. Examples of social engineering attacks.
   1. Access to a building can e.g. happen through
      - tailgating behind others, e.g. after lunch break, or with cigarette smokers,
      - carrying heavy boxes and getting helpt to open door
      - producing and presenting a fake access card
   2. Installing malware on the computer of CEO can e.g. happen through:
      - Sending customized spear-phisning email with attached malwar to be installed and executed,
      - Sending customized spear-phishing email with attachment or link to website that contains an exploit of a zero-day vulnerability that is present on the CEO's computer.
b. A false positive is when a legitimate authorized person is challenged. A false negative is when an attacker is not identified.
c. The analogy to configuration firewalls would be to organize awareness training on the appropriate policy and practice to people about how to detect and react to social engineering attacks.