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.

Answer

a. Published 27K standards
   1. 27000 — Information security management systems — Overview and vocabulary
   2. 27001 — Information security management systems — Requirements
   3. 27002 — Code of practice for information security management
   4. 27003 — Information security management system implementation guidance
   5. 27004 — Information security management — Measurement
   6. 27005 — Information security risk management
   7. 27006 — Requirements for bodies providing audit and certification of information security management systems
   8. 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
   9. 27031 — Guidelines for information and communications technology readiness for business continuity
   10. 27033-1 — Network security overview and concepts
   11. 27035 — Security incident management
   12. 27799 — Information security management in health using ISO/IEC 27002

b. 27K standards in preparation
   13. 27007 — Guidelines for information security management systems auditing (focused on the management system)
   14. 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)
   15. 27013 — Guideline on the integrated implementation of ISO/IEC 20000-1 and 27001
   16. 27014 — Information security governance framework
   17. 27015 — Information security management guidelines for the finance and insurance sectors
   18. 27032 — Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
   19. 27033 — IT network security, a multi-part standard based on ISO/IEC 18028:2006 (part 1 is published already)
   20. 27034 — Guideline for application security
   21. 27036 — Guidelines for security of outsourcing
   22. 27037 — Guidelines for identification, collection and/or acquisition and preservation of digital evidence

c. Drivers behind standards can be:
   - a real need for a new standard,
   - personal interest/ambition/vanity of individuals to be recognised as international security expert.

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. the security management within an organisation. ISO/IEC 27002 is a check list of security contorols, i.e. possible practical security controls.
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

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

Answer

- Plan (establish the ISMS). Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organisations overall policies and objectives
- Do (implement and operate the ISMS). Implement and operate the security policy, controls, processes and procedures
- Check (monitor and review the ISMS). Assess and where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.
- Act (maintain and improve the ISMS). Take corrective and preventive actions based on the results of the management review to achieve continual improvement of the ISMS.

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?

Answer

a. Examples of definitions of social engineering:
   - The act of tricking another person into providing confidential information by posing as an individual who is authorised to receive that information (Harris, p.967).
   - The process of deceiving people into giving confidential, private or privileged information or access to a hacker. (David Gregg, "A Multi-Level Defence Against Social Engineering")
   - The art of influencing the behaviour of a human victim to breach security without the victim even realising that they have been manipulated. (Radha Gulati "The Threat of Social Engineering and Your Defence Against it")
b. SE attack strategies:
   - Develop trust
   - Induce strong affect
   - Reciprocation
   - … and others, see lecture slides
c. A false positive is when a legitimate authorized person is challenged. A false negative is when an attacker is not identified.
d. The analogy to firewall configuration would be to teach the appropriate policy and provide practical training to people on how to detect and react to social engineering attacks.

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?

Answer

a. Physical access control is not enough when physical access to equipment and resources can not be prevented, and when access can only be given remotely through computer networks.
b. Physical access control mechanisms include walls, gates, locks, guards, etc
c. Physical security needs to be implemented based on a layered defence model. If one layer fails, other layers will protect the valuable assets. (Harris, p.339). The layers can for example be called 1) perimeter security, 2) building entry security and 3) interior security.

QUESTION 6

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

Answer

a. CPTED: Crime Prevention through environmental design
b. The crux of CPTED is that the physical environment can be manipulated to create behavioural effects that will reduce crime and the fear of crime. It looks at the components that make up the relationship between humans and their environment. This encompasses the physical, social, and psychological needs of the users of different types of environments and predictable behaviours of these users and offenders.
c. The main principles used in CPTED are:
    - Natural Surveillance
    - Natural Access Control
    - Territorial Reinforcement
    - Activity Support
    - (Target Hardening, not really part of 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.

Answer

BS 7799, which was the original version of ISO 27002, contained 10 sections of security controls. A new section was added to ISO 27001 which therefore has 11 sections of security controls. Similarly, CISSP has 10 domains of CBK (Common Body of Knowledge).Some of the sections/domains are more or less the same, but some are specific to either ISO 27002 or CISSP CBK, so there is no 1-to-1 mapping between the two documents.

Digital Forensics and Cyber Security are quite relevant today, but are not mentioned in any of them, probably because they were not seen as relevant when ISO 27002 / CISSP CBK were defined.