The Elements of a Security Management System

By Per Rhein Hansen, M.Sc., Ph.D., Post Danmark, Internal Audit - phn@post.dk
External lecturer at the IT University of Copenhagen

Abstract

The term “security” is in fact misleading because such a thing does not exist in real life! Our aim is to obtain security to some extent but we are only able to try to protect ourselves and our IT resources against the threats we know are present. Therefore, in both the private and the public sector, top management has to apply a close monitoring program on threats and vulnerabilities related to the systems. In fact, recognition is gradually emerging on the need for an IT-security Management System of the kind we know as “Quality Management Systems” (ISO 9000) or “Environmental Management Systems” (ISO 14001). In this paper the elements of a security management system will be presented.

When we are convinced the necessary rules, procedures, and instructions as well as technical security mechanisms have been installed, we must be aware that compromises might have been introduced (for example “holes” through the firewall) deliberately or accidental. Employees / users make mistakes, forget instructions, or even circumvent troublesome security measures. This situation is aggravated by the difficulties observed in performing the necessary protection engineering to the constantly changing computing environment.

How to obtain the right security level? First and foremost we have to establish an “IT Security Management System” which should be the base for effective handling of all security activities, whether proactive or reactive. This base includes a series of well-known management disciplines in a recurrent flow:

1. Directing
2. Organising
3. Risk assessing
4. Planning
5. Implementing
6. Training
7. Operating
8. Monitoring
9. Evaluating
10. Correcting

Below is an element by element description:
1. DIRECTING
Management direction and commitment are necessary preconditions for obtaining IT-security throughout the organisation. Direction is given through overall guidelines - and committed to through an IT-security program including
- IT-security policy as a basis for responsible behaviour with overall security objectives of the organisation as well as a statement on allocation of responsibilities.
- IT-security strategy depicting how the objectives are to be fulfilled
- Employee training program to obtain increasing awareness and understanding concerning IT-security

2. ORGANISING
A management structure is required to control the entire cycle of IT-security activities and roles have to be defined.
- A steering committee to guide and monitor the IT-security activities within the organisation
- The IT-security responsibilities of line management are specified
- The IT-security officers functional duties are specified
If an existing management forum is ready to take care of these activities a special steering committee is not mandatory.

3. RISK ASSESSING
The business risks should be managed to obtain a consistent and acceptable security level.
- It is management responsibility to recognise the threats and risks to the business / organisation and to introduce the necessary but cost effective counter-measures
- Proper tools for risk evaluation should be available
- Risk assessment should be discussed regularly by the steering committee as part of its overall evaluation of security management procedures including correct guidelines, and the way they are adhered to.

4. PLANNING
Security measures should be planned according to the business needs defined during the risk assessment
- Based on the identified risks a necessary set of counter-measures are specified. For the measures to be coherent and complete it might be advantageous to establish an IT-security architecture
- Implementation projects are defined and planned

It might be considered to apply a “baseline security approach” by which a minimum set of safeguards appropriate for a certain level of risk is implemented - without a prior
detailed risk analysis. This viewpoint is supported by a guideline named Technical Report ISO/IEC TR 13335. However no agreement has been reached on what is a minimum set of safeguards. Today the UK has a British Standard 7799 “Code of Practice for Information Security Management” (now an international standard), Germany has an “IT Baseline Protection Manual”, and Denmark has a Danish Standard for IT-security DS 484 (which is heavily based on BS 7799).

Special considerations should be given to the selection of safeguards when an organisation connects its internal network to external networks, e.g. Internet. Some guidelines are given in the TR 13335-5 which currently is only at the draft level.

5. IMPLEMENTING
Security measures are implemented in the form of technical mechanisms and administrative procedures. According to ISF (Information Security Forum) an international association of over 240 leading organisations providing de facto standards to its members, they should at least cover the following areas:

- Security Management
- Critical Business Applications
- Information Processing
- Communications Networks
- Systems Development

6. TRAINING
This element must not be neglected because the human part of IT-security is decisive for the outcome of a total IT-security program

- Awareness-raising and training programs to obtain commitment for IT-security throughout the organisation
- Availability of relevant external training (tutorials, seminars or conferences) for key employees

7. OPERATING
The day to day activities should follow procedures, incidents must be dealt with, and data files must be backed up during operations. Especially important is the existence of

- Configuration management, i.e. the process of keeping track of changes to the system
- A change management procedure which is used for identifying new security requirements when IT systems change
- A problem management procedure
- Backup and disaster recovery procedures

8. MONITORING
As part of the IT-security management cycle, management must be able to obtain a clear view of achievements compared to the original targets

- Reviewing whether the measures and procedures are implemented as intended and are complied with
- Reviewing changes to the environment and the technical infrastructure as they may have rendered the safeguards ineffective
- Possibly installing a self-assessment program
- Possibly making use of independent “third party” reviews against commonly accepted standards

9. EVALUATING
The monitoring process results, especially the deviations, should be reported to management on a regular basis - and an evaluation of the achievements performed to determine if they have been satisfactory or if the IT-security policy needs tuning

- Management examine the review and assessment reports for the past period
- As basis for the evaluation an updated risk evaluation is acquired
- Management decides on the appropriate actions to be taken

10. CORRECTING
If corrections are deemed necessary, initiatives are prioritised and resources are allocated

- The IT-security policy should be updated
- The IT-security strategy is changed according to new priorities
- Necessary implementation projects are initiated

This sequence of 10 activities is now repeated in a recurring cycle of 6 to 12 months. This way top management will be able to participate directly in the steering process without too much effort. And the employees will have the necessary guidance and updated specifications for their day-to-day work.

If a security management system is established this way, we should have no more problems. However many companies / institutions will still have problems because they are not able to continuously focus on all 10 elements of the management cycle at the same time. We have to realise that just a single breach or weakness within one of the elements will jeopardise the entire management system. “The weakest link determines the strength of the whole chain”.

The weakest link is often seen as “Risk Assessing” because it is a cumbersome and complicated activity and proper tools are not allways available. Nevertheless, it is one of the most important activities. Fortunately well described methods have recently appeared, e.g. the document “PD 6668:2000 Managing Risk for Corporate Governance” from the British Standards Institute where a “Process for identifying business threats and risks” is presented.
In fact both BS 7799 and DS 484 supports a procedure that includes risk assessment at the overall level and the assessment results are considered as the basis for the selection of security measures and controls.

Still, the most important contribution to the security management cycle is that top managers or steering committee members involve themselves continuously to make sure that all the elements are functioning at all time.

Finally, primarily in the finance sector, the IT-auditors should make sure that the management and steering committee performs according to policy and procedures (the management cycle). This kind of assessment must be based on hard evidence and deviations should be reported to the board of directors.