Security Assessment and Planning in Small Organizations

O.Mazhelis and H.Isomäki

Information Technology Research Institute, University of Jyväskylä, Finland
e-mail: mazhelis@titu.jyu.fi, hannakaisa.isomaki@titu.jyu.fi

Abstract

Information security is one of the major concerns in contemporary organizations, and these organizations devote significant portion of their resources in order to identify and mitigate their security risks. A number of formal methods can be used to support the process of security risk assessment and planning; however, these methods are usually aimed at large or medium organizations. Meanwhile, the resources available in smaller organizations may appear insufficient for applying a full-scale assessment and planning method, and, therefore, these methods should be tailored first to the constraints present in an organization. This paper introduces a derivative of a well-known security assessment and planning method adjusted to the needs of small organizations, and reports on the use of this method in a small organization.

Keywords

Information security management, small and medium enterprises

1. Introduction

Information technologies (IT) have become an indispensable attribute of our society, and organizations more and more rely on IT support in their businesses. As the involvement of IT in various business activities increases, it becomes also more important for the organizations to systematically manage information security, i.e. to assure the availability, integrity, and/or confidentiality of the information processed by their computer systems. The importance of security may stem from the need to meet customer's expectation or otherwise satisfy business requirements, from the need to comply with legislation, etc.

An important part of the information security management is the assessment of the current situation within the organization (risk assessment), and incremental improvement of the situation (risk mitigation). To make the assessment and mitigation of information security risks more systematic, organizations may apply risk management methods available in a form of security standards (ISO/IEC 7498-2, 1989; ISO/IEC 17799, 2005; ISO/IEC 21827, 2002; ISO/IEC 15408, 2005) and frameworks, e.g. Federal IT Security Assessment Framework (Chief Information Officers Council, 2000), OISSG ISSAF (Rathore et al. 2007), CMU/SEI OCTAVE (Alberts et al. 2003), ITGI COBIT (CobiT, 2007). Some of these methods (e.g. NIST Common Criteria (ISO/IEC 15408, 2005)) deal with the security of IT products and systems, while the others focus on the security-related processes in organizations, ranging from semi-formal guidelines and best practices (ISO/IEC 17799, 2005) to formal quantitative and qualitative methods (Alberts et al. 2003; Hamdi and Boudriga, 2003).

The available security risk management methods are targeting mainly large enterprises. For instance, OCTAVE method is targeting the organizations with 200+ people, and even its smaller-scale variation OCTAVE-S (Alberts et al. 2003) is aimed at organizations with up to 100 people. These methods are rather extensive and complex, and significant amount of organizational resources need to be devoted to the security assessment and planning. As a result, applying these methods in small organizations may be impractical, since the resources needed for the method implementation may be prohibitively large given the small size and scale of operations of the organization.

Meanwhile, security assessment and planning is vital also in smaller organizations which play a crucial role in the European economy and the Western society in general. Indeed, small and medium enterprises (SME) having less than 250 employees account for over 99% of the number of enterprises and offer workplaces to almost 70% of those employed in private sector (Audretsch et al. 2003). In turn, small and micro enterprises, i.e. those with 10 to 49 and 1 to 9 employees respectively, represent a vast majority of European SMEs – 6.5% of SMEs are small ones, 92.5% are micro, while only 1% are medium sized enterprises. To the best knowledge of the authors, available security assessment and planning methods do not address the demands and limitations of such small organizations, and therefore, there is a need for adjusting these methods, in order to make them applicable in these organizations.

This paper focuses on the security assessment and planning in small organizations. In the paper, we introduce a small-scale method for security assessment and planning which is derived from OCTAVE-S and is targeting small (50 employees and less) organizations. This method has been successfully applied in a small Finnish organization. The paper provides the details of the method, and describes its successful application in the organization.

The remainder of the paper is organized as follows. In the following section, the motivation for the method elaboration efforts is given, while the details of the proposed security assessment and planning method are provided in Section 3. Section 4 describes the application of the method in a case organization. Finally, conclusions to the paper are provided in Section 5.

2. Motivation and related work

In the next section, a method for security assessment and planning in small organizations is introduced. Prior to the introduction of the method, let us consider some of the general requirements that such a method should meet:

- The method should support systematic risk assessment and mitigation planning.
- It should be applicable to small enterprises having 50 employees and less.
- It should be applicable to organizations with different information security needs and with different degrees of information security development.

A number of standards and frameworks can be applied in order to make the process of security management more systematic. Some are targeted at the *systems* security

evaluation – e.g., ISO 15408 NIST Common Criteria provides a structural approach to the evaluation of how IT products and systems match their security requirements. As such, this standard focuses on the security of IT products and systems rather than organizations. A number of methods are also available for the security assessment at the *organizational* level; some of them are described in Table 1.

Method name	Description
ISO 7498-2 (ISO/IEC 7498-2, 1989)	introduces the basic concepts of information security management including security goals, security services that should be provided in order meet these goals, and security mechanisms implementing the above services.
NIST 800-30 Risk Management Guide for Information Technology Systems (Stoneburner et al. 2002)	aligns risk management, consisting of various risk assessment and risk mitigation activities, with the system development lifecycle including the initiation, development or acquisition, implementation, operation or maintenance, and disposal phases.
ISO 17799 Code of Practice for Information Security Management (ISO/IEC 17799:2005, 2005)	provides a set of best practices for managing information security and categorizes them into twelve categories. Within each category, security objectives and relevant security controls are described, while the standard provides no recommendations as to which specific controls are to be implemented.
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Alberts et al. 2003)	is an asset-driven security risk evaluation method. The evaluation is done in three phases: i) identification of assets, requirements, threats, and vulnerabilities; ii) identification of technological vulnerabilities for critical assets; and iii) assessment of the security risks aimed at deriving the areas for improvement.
Control Objectives for Information and related Technology (CobiT, 2007)	is an enterprise IT management framework which offers a general process model for organizing IT activities; part of these activities are security-related.
Federal IT Security Assessment Framework (Chief Information Officers Council, 2000)	describes an approach to determine the status of IT security in an organization as matched against its security objectives, and to define targets for improvements. For the organization's information and system assets, the framework establishes five levels of asset security, and offers the criteria to determine whether the specific level is adequately implemented.
ISO 21827 Systems Security Engineering Capability Maturity Model (SSE-CMM) (ISO/IEC 21827:2002, 2002)	is a process reference model for the organizations involved in information security engineering: product developers, service providers, system integrators, etc. It is aimed at the evaluation of the product or system engineering activities spanning the whole lifecycle of the system/product being developed. The model introduces six maturity levels ("no security" level and five levels of information security maturity).

Table 1: Methods for security assessment at the organizational level

The above methods can be classified into the methods based on generic checklists (e.g. ISO 17799 or COBIT Quickstart) and the method based on tailored security models (e.g. NIST 800-30 Risk Management Guide). The former assume that a roughly same set of mitigation activities are required in a majority of organizations, and therefore the information security in an arbitrary organization may be assessed by routinely comparing the current situation with the checklist. The latter consider each organization as unique, and attempt to construct the risk-driven model describing security assets, threats, and countermeasures particularly fitting the

context of each organization. Some methods, such as OCTAVE and Federal IT Security Assessment Framework, strive to combine both of these approaches.

The methods above are aimed at large organizations (though some variations aimed at smaller enterprises, e.g. COBIT Quickstart or OCTAVE-S, are available). Their wide scope and high complexity make their use impractical in small organizations with highly limited resources. Therefore, in order to support security assessment and planning in small organizations, a method tailored to the needs of such small organizations is introduced in this paper.

The combined methods are more flexible and hence may adjust better to the needs of a particular organization. Furthermore, among the combined methods, OCTAVE provides a smaller-scale variation OCTAVE-S applicable to medium sized enterprises (Alberts et al. 2005). Therefore, the OCTAVE-S method has been chosen as a base for our security assessment and planning method.

The OCTAVE-S method follows a risk-based strategic assessment and planning approach to security, and is tailored to organizations with up to 100 people. It consists of five processes and 17 activities organized in three phases. In the first phase, organizational assets are listed; their security requirements are stated, and the threats to and vulnerabilities of these assets are identified. (An asset is defined in OCTAVE-S as “something of value for the organization”, a threat is defined as “an indication of a potential undesirable event”, and an impact represents “the effect of a threat on an organization's mission and business objectives”.) The second phase focuses on the identification and analysis of technological vulnerabilities for critical assets. Finally, in the third phase, areas for improvements are derived.

As compared with the base OCTAVE method, the OCTAVE-S has two differences (Alberts et al. 2005). First, it avoids the need for extensive data gathering and other workshops by employing a small group of three to five people who are assumed to possess a deep knowledge of the organizations' processes. Second, it scales down the technology vulnerabilities analysis, to match limited resources of smaller organizations. The activities and their order are also somewhat different from the base OCTAVE method.

3. Small-scale security assessment and planning method

The process of risk-driven security analysis in the proposed method has similarities to the OCTAVE-S method. Similarly, the asset-based threat profile is created and then used to evaluate the risks associated with different assets and threats. However, in our method, we further scale down the phases and activities of the OCTAVE-S to meet the needs of a small organization. The main differences between the OCTAVE-S and the proposed method are described below:

- First of all, we avoid the assumption in OCTAVE-S that a team of three to five people with deep understanding of the company is available. Instead, it is assumed that two to three experts with overlapping knowledge of the organization's processes and practices are available. Besides, a person

knowledgeable of the method but not necessarily possessing a deep knowledge of the organization (potentially an external consultant) is responsible for performing the major part of the activities, while the experts are mainly used in order to provide information and refine the results.
- Second, while OCTAVE-S mixes the identification of the security needs of the organization with the evaluation of its current security level, we assume that, as the organization develops, its security level improves faster than the security needs of the organization are changing. Therefore, to make the security needs reusable in subsequent rounds of analysis, in our method, the identification of the security needs and the evaluation of current security level are kept separate.
- Whenever possible, the activities of the analysis are simplified.

In the remainder of the section, the details of the proposed method are provided. The method can be divided into three phases: i) identification of security needs of the organization, ii) assessment of the current situation with respect to the identified needs, and iii) identification of the areas for improvement. The subsections below describe these phases.

3.1. Identifying security needs

In the first phase, the asset-based threat analysis is performed. The purpose of this phase is to list the organization's critical assets and their security requirements, to identify threats to these assets and the impact of these threats if materialized, and to outline possible mitigation approaches. The following processes are included in the analysis (in Figure 1, the information flow between the processes is shown):

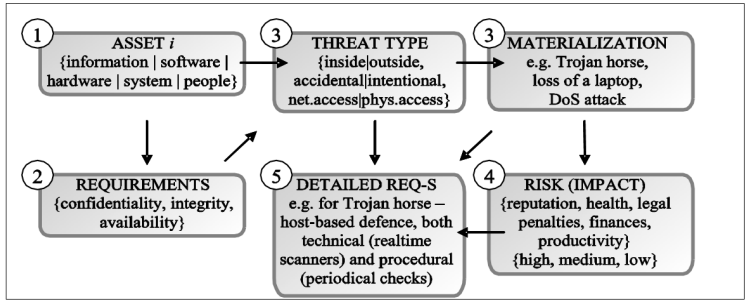

Figure 1: Asset-based threat analysis

- *Preparation*. The purpose of this initial activity is to set an agreement, between the person responsible for carrying out the method (hereafter the leader) and the group of IT experts (hereafter the expert group) on the details of the method. The method's details are also discussed with the organization's management, to assure management support for the activities to be undertaken.
- 1. *Identifying assets and their relative importance*. Representatives of different stakeholder groups are interviewed by the leader, in order to identify information, software, hardware, and systems assets. A summary of these interviews, along with the other documentation available in the organization (inventory of equipment, network map, etc.) are used in order to outline

important organizational assets. After that, a meeting with the expert group is held in order to prioritize the assets, and identify (five to ten) critical assets.

- 2. *Identifying security requirements for the critical assets*. For the *important* assets, their security requirements are formulated by the leader in abstract form, i.e. in terms of the high, medium, or low need for confidentiality, integrity, and availability. In a workshop with the expert group, these requirements are discussed; for the critical assets, operational requirements are formulated.
- 3. *Hypothesizing the threats to the critical assets*. For each *critical* asset, potential threats, such as system errors or human access (intentional or accidental, physical or network) are described; the description of a threat includes possible ways of its materialization. The description is first done by the leader, and then is discussed and refined with the help of the expert group.
- 4. *Estimating the risks to the assets*. Here, only one aspect of the risk (namely, impact) is analyzed, while the analysis of other aspects (exposure rate, vulnerability to the threat) are not taken into account. In this process, the leader is responsible for i) defining the impact criteria including areas of impact and degrees of impact, and ii) hypothesizing the impacts of different threats. As in the other processes, the results are discussed and refined in a workshop with the expert group. As a result of the process, threats of high impact are defined.
- 5. *Outlining detailed requirements in a form of mitigation activities*. Possible technical and procedural ways to mitigate threats are identified. For small-impact threats, a decision to defer the mitigation or accept the risk may be made. The identified mitigation activities can be seen as detailed security requirements.

Thus, as a result of this phase, the baseline of security requirements is set. These requirements formulated as mitigation activities will be refined in the next phase by utilizing the checklist of the best practices.

3.2. Assessing current situation and complementing mitigation activities

The purpose of this phase is to determine how well the organization's security needs, formulated as mitigation activities, are fulfilled by its present technical and procedural measures, and to complement these activities with the help of checklists.

In this phase, a workshop is held, where the expert group considers the list of defined mitigation activities and assesses to which extent these activities are implemented in the organization. Prior to the workshop, the security of configurations in organization's critical software and systems assets is examined using appropriate tools.

Some potentially useful mitigation activities may be overlooked in the course of the asset-based threat analysis. To complement the list of mitigation activities, in this phase, a checklist of best security practices available in OCTAVE-S (Alberts et al. 2001) is consulted. A separate workshop is organized, where the expert group completes the security practices survey (Alberts et al. 2005) aimed at determining whether (and to which extent) these practices are in use in the organization. For those practices which are not used systematically, a preliminary decision is made about the need to adopt the practice in the organization.

As opposite to the first phase, the expert group plays an active role in this phase, while the leader is responsible for guiding the process, and actively participating in the examination of the configurations of critical software and systems assets.

3.3. Specifying security to-do items

The activities in this phase base upon the results of threat analysis and current situation assessment performed in two previous phases.

In this phase, the mitigation activities derived from the threat analysis and the activities defined based on the security practices survey are aggregated. All the activities corresponding to the threats with high or medium impact should be included, while the activities for the low-impact threats may be optionally excluded from the aggregated list. Furthermore, more concrete to-do items may be specified for some of the mitigation activities. For instance, for the activity "Implement a mechanism for propagating information about important security issues", a possible to-do item may be "Publish less critical warnings on a dedicated Intranet page".

The aggregation of the mitigation activities is carried out by the leader. After that, a series of workshop with the expert group is held, during which the activities are refined, and the to-do items are specified. Also, the individuals responsible for implementing the items and their time span are specified. Finally, the results are brought to the management for discussion and approval.

3.4. Iterative approach

The overall information security management can be seen as a repeating Deming cycle of plan-do-check-act activities (Tague, 2004); in this cycle, the security assessment and planning method covers mainly the planning part and partly the acting part. Therefore, a successful use of the method assumes that the other activities, namely those covering do, check, and act parts of the cycle, are undertaken by the organization as well. Furthermore, it assumes that the method is to be iterated, either on a regular basis or whenever a change in organization's security needs occurs.

It is worth mentioning that, since the identification of security needs and the assessment of the current security level are kept separate in the method, the subsequent iterations of the method execution is likely to be easier as long as the security needs remain unchanged – in this case, only the security level needs to be reassessed, and hence the efforts required for the assessment are likely to be reduced.

4. Method application in practice

The security assessment and planning method described in the previous section has been applied in a small organization. The case organization represents a small research and development unit operating independently within a large Finnish organization. It is a project-based organization, where most of the personnel are working for specific projects funded by external sources. These projects are carried out in collaboration with industrial partners as well as with other national and

international research units. The staffing of the organization fluctuates between 40 and 60 employees, depending on the needs of projects.

Organization's IT, managed by an internal information management group (IMG), play a critical role in the organization's operations:

- For many (if not all) projects, daily work requires the use of IT for communication, information search, and document preparation.
- Some of the projects involve development and provision of services for partner organizations; these services are Internet-based and require IT infrastructure.
- Projects often include software development in their tasks; the software development processes naturally rely on the presence of IT infrastructure.
- The results of the project work are stored in electronic form for further reference.

Thus, reliable and swift IT support is needed for the normal operations of the organization. A critical aspect of managing IT in it is information security management: the systems and information should be available, and the confidentiality of information, as required by the contractual agreements with partner organizations and other regulations, needs to be ensured. Diverse requirements of different projects make the problem of managing security more difficult. Meanwhile, in past, the management of information security was done by the IMG rather semi-systematically: various security practices were implemented routinely, while only some of them were documented; security planning was done in an ad-hoc way resulting in a set of practices apparently covering only a subset of the organization's security needs, etc.

With the aim to improve the situation, a systematic security assessment and planning has been performed using the method described above. For this purpose, the organization hired one person to be responsible for the method execution; besides, the members of the IMG were made available for the assessment and planning activities.

As a result of the security assessment and planning, 84 classes of assets were listed in total; among them, 29 were found important, and out of those, 8 were identified as critical assets. Having formulated operational security requirements for each of the critical assets, threats to these assets were analyzed, and appropriate mitigation activities were defined. These were extended with further activities as suggested in the catalogue of best practices. After aggregation, a total of 132 mitigation activities in 15 mitigation areas were produced, and 83 to-do items were specified. The following deliverables have been produced: i) threats analysis report including a list of assets, threats and their impacts, and mitigations activities, ii) security requirements report providing general mitigation activities as well as asset-specific mitigation activities along with the relevant to-do items, and iii) auxiliary documents such as security practice survey results, summary of interviews, and other working documents.

The security assessment and planning itself took place in the autumn of 2006, and the whole process spanned over the period of three months. In addition to the leader, three members of the IMG actively participated in the process playing the role of the expert group. Table 2 summarizes the resources spent for the purposes of executing the method.

Phase	Events and participants	Time span
1	15 interviews, 3 workshops (leader and expert group)	5 weeks
2	1 workshop (expert group)	1 week
3	7 workshops (leader and expert group)	6 weeks

Table 2: Use of resources for security assessment and planning

As could be seen from the table, the second phase included only one workshop devoted to the security practices survey; this is because the second workshop belonging to this phase was merged with the last workshop of the first phase.

Due to the time limitations of expert group members, each workshop lasted in average only 1.5 hours; two or three members of the expert group were present. Besides, each of the expert group members devoted roughly three working days to commenting and refining the working documents produced in the course of the assessment and planning. Thus, the overall effort by the expert group is approximately 15 person-days, or equally three person-weeks.

Each of the interviews conducted in the first phase of the project lasted in average 45 minutes, i.e. about 1.5 person-days were spent by the employees for the interviews. Finally, the leader was involved in the security assessment and planning during its whole duration for approximately 70% of time, hence totalling 8.4 person-weeks. Thus, the total efforts amounted for approximately 12 person-weeks, which is a quite promising result given the wide scope of the assessment and taking into account the fact that the participants had no previous experience with the method. In the further applications of the method, the efforts may be also decreased as the templates created in the assessment and planning process can be reused.

5. Conclusions

Systematic information security assessment and planning is a crucial element of information security management in organizations. While a number of assessment and planning methods are available in literature, applying them in small organizations may be impractical, due to the overwhelming efforts that may be needed if a method is applied directly.

In this paper, a small-scale security assessment and planning method aimed at supporting security management in small organizations is introduced. The paper provides the details of the method, and describes its successful application in a real small organization. The use of the method in the case organization has allowed this organization to systematically formulate its security needs, assess the current security level, and identify the mitigation activities to be undertaken. The real-world experience with applying the proposed method suggests that moderate efforts totalling three person-months are required for the method execution, thus making it applicable in small organizations having only a few dozens of employees.

Derived from the well-known OCTAVE-S method, the proposed method matches the OCTAVE criteria of being self-directed, flexible, continuous-process driven,

forward looking, etc. (Alberts et al. 2003). The method separates the identification of organizational security needs and the assessment of the current security level. Such separation is aimed at making the subsequent iterations of the method execution easier – if the security needs remain unchanged, only the security level needs to be reassessed. As a result, the efforts required for the assessment are likely to decrease.

So far, the proposed method has been applied only in one organization. Therefore, further testing of the method in different organizational settings is necessary; for this, further application of the method in other organizations along with the refinement of the method's processes and activities is required. In order to reduce the efforts required for the method execution, and thereby make it applicable in even smaller organizations, also further work on developing generic templates and tools is needed. Moreover, end user security behaviours need to be added and tested as parts of the method. Special attention will be paid to identifying factors of ICT use that form the most essential risks in SME's information security, and to the factors by which these behaviours can be prevented or managed.

6. References

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), *Introduction to the OCTAVE Approach*, The Software Engineering Institute, Carnegie Mellon University. Available from www.cert.org/octave/methods.html.

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2005), *OCTAVE-S Implementation Guide*, Version 1.0 (CMU/SEI-2003-HB-003), The Software Engineering Institute, Carnegie Mellon University. Available from www.cert.org/octave/osig.html.

Alberts, C. J., Dorofee, A. J. and Allen, J. H. (2001), *OCTAVE Catalog of Practices*, Version 2.0 (CMU/SEI-2001-TR-020), The Software Engineering Institute, Carnegie Mellon University. Available from www.cert.org/octave/pubs.html.

Audretsch, D. B., Thurik, A. R., Kwaak, T. and Bosma, N. (2003), SMEs in europe 2003", *Observatory of European SMEs*, No. 7.

Chief Information Officers Council (2000), *Federal Information Technology Security Assessment Framework*, NIST, Computer Security Division, Systems and Network Security Group. Available from csrc.nist.gov/organizations/guidance/.

CobiT (2007), *COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*, Published by The IT Governance Institute (ITGI) and Information Systems Audit and Control Association (ISACA).

Stoneburner, G., Goguen, A. and Feringa, A. (2002), *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, Springfield, VA.

Hamdi, M. and Boudriga, N. (2003), Algebraic specification of network security risk management, in "*FMSE'03: Proceedings of the 2003 ACM workshop on Formal methods in security engineering*", ACM Press, New York, NY, USA, pp. 52–60.

ISO/IEC 15408 (2005), Information technology – Security techniques – Evaluation criteria for ITsecurity, ISO, Geneva, Switzerland. Second edition. Available from isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm.

ISO/IEC 17799:2005 (2005), Information technology – Security techniques – Code of practice for information security management, ISO, Binarynine Limited, United Kingdom.

ISO/IEC 21827:2002 (2002), Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM), ISO, Geneva, Switzerland. Available from isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm.

ISO/IEC 7498-2 (1989), Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security architecture, ISO, Geneva, Switzerland.

Rathore, B., Brunner, M., Dilaj, M., Herrera, O., Brunati, P., Subramaniam, R. K., Raman, S. and Chavan, U. (2007), *Information Systems Security Assessment Framework* (ISSAF) Draft 0.2.1B, Open Information Systems Security Group. Available from www.oissg.org/issaf.

Tague, N. R. (2004), *The Quality Toolbox*, second edn, ASQ Quality Press.