

A MODEL FOR EXPLAINING STRATEGIC IT- AND INFORMATION SECURITY TO SENIOR MANAGEMENT

JOHN LINDSTRÖM
Luleå University of Technology
Sweden
john.lindstrom@ltu.se

ANN HÄGERFORS
Luleå University of Technology
Sweden
ann.hagerfors@ltu.se

Abstract

Awareness and understanding of strategic IT- and information security appears to be a low priority amongst senior managers although this falls within their responsibilities. In this paper a tested and confirmed model used to explain strategic IT- and information security is described. The model has been iteratively developed and applied in development, implementation or training in five different organizations. In these five cases, senior management awareness and understanding of strategic IT- and information security was verified as being very low. The model was originally developed to explain IT- and information security to corporate senior management. It has been adapted for use in the public sector by changing some of the terminology to match that used within the public sector. The model may also be used for training purposes, with regards to senior management or personnel in strategic IT- and information security. The importance of senior management ownership and care for strategic elements of the organization's security programme is also discussed and the conclusion drawn is that the operative levels should be coordinated by one or a few members of the senior management team.

Keywords: strategic IT- and information security, senior management, security programme

1. Introduction

The problem addressed in this paper is that senior management (top management) appears to lack awareness and understanding of strategic IT- and information security. By *strategic* we mean strategic instruments to steer an organization that fall under the responsibility of senior management. The term *IT- and information security* can be viewed as an entity of security for both IT and information [Harris, 2004]. Strategic IT- and information security form part of the strategic steering instruments for senior management [Anttila et al., 2004; Wylder, 2004], but are often not cared for properly [Kajava et al., 2006]. Decisions with regards to strategic IT- and information security should not, for convenience sake, be delegated to only one member of senior management or to the IT-department or a similar department. For the majority of organizations, IT- and information security for have an increased importance and thus

there is a necessity to integrate the strategic parts into the senior management agenda on a continuous basis in order for these aspects to be maintained and looked after [Anttila et al., 2004; Wylder, 2004; Leveque, 2006].

The discussions in Kajava et al. (2006) are that top managers often possess only a superficial understanding of information security which may lead them to make decisions that are not conducive to raising the organization's security level. It was also mentioned that only 20% of managers realized that information security was of strategic value to their companies. They stated that enhancing the information security awareness among all employees had been found to be necessary, but that the key to success was to raise the awareness level of senior management – who have often shied away from any training with regards to these matters. This lack of awareness and understanding has been confirmed in the development, implementation, and training for strategic elements of IT- and information security at a number of corporations and government agencies. This poor understanding often has an adverse effect on the ownership, care and thus, in addition, on any upcoming results.

Kajava et al. (2006), Lempinen (2002), Wylder (2004) and Leveque (2006) state that commitment from senior management to information security is of utmost importance in order to pave the way towards the information society, and they recommend that a member of senior management should be responsible for coordinating the organization's information security strategy. Senior management should own and spend time on all the strategic parts of the business, as strategic decisions do have an effect on the operational decisions in an organization at the lower levels if work proceeds in a top-down manner. Further, they state that the key component of information security work is the viable support and engagement of senior management, by for instance participating in information security related events.

Kolkowska (2005) discusses that taking information systems security in modern organizations seriously requires more than that on offer from traditional technology-centred security approaches, and that relevant socio-technical aspects such as individual and organizational values are equally important. It is further stated that the behaviour of the employees of such organizations is difficult to formalize by rules, procedures and regulations and sometimes the relevant rules are missing. Wylder (2004) and Leveque (2006) discuss the importance of building values and a culture which also consists of information security aspects. Hofstede (1990) describes with the following model, see figure 1, that the most important aspect of an organization's culture is its values, and that symbols, myths and rituals can be considered as practices. This paper will continue to build on the work in [Kolkowska, 2005; Hofstede, 1990] using the organizational values as part of the strategic elements of IT- and information security.

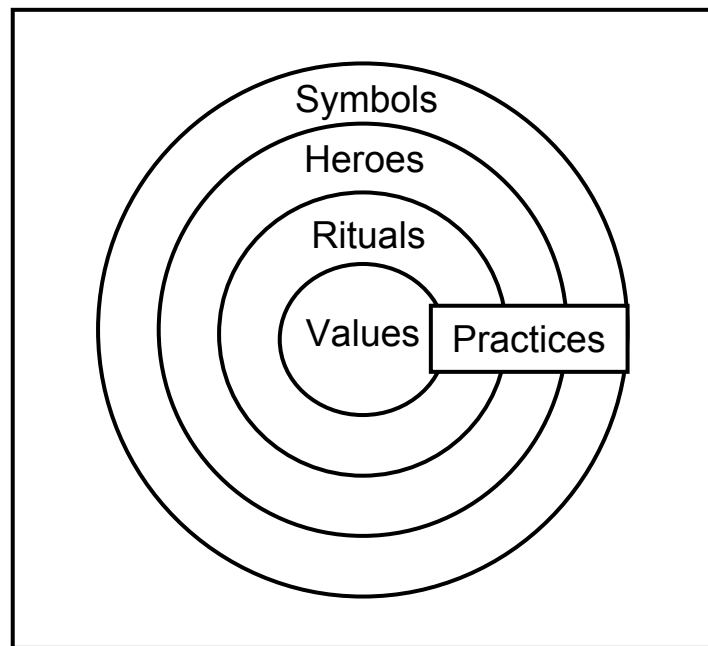


Figure 1. Manifestations of culture: From shallow to deep [Hofstede, 1990].

IT- and information security must form an integral part of the Business Continuity Planning. A great deal has been written about Business Continuity Planning such as in NIST with Swanson et al (2002), ISO/IEC 17799 (2005), the Swedish Emergency Management Agency's (2006) framework "Basic Level for Information Security" called BITS, report from the Swedish Finance Inspection (2005), and Lam (2002) regarding how to organize and develop Business Continuity Planning and what must be considered in order to maintain it. What is not mentioned in these texts is how the Business Continuity Planning fits into the management of an organization and the overall business planning and why senior management should own and care for the Business Continuity Planning.

Grimalia (2004) discusses how to train students with regards to information security, also mentioning that later on in life security practitioners need technical, social and political skills (to be able to "sell" information security to senior management). It also states that awareness and educations are the keys to the success of a security programme's overall success.

There are a number of standards and frameworks that can be used to create a security programme (that is sometimes also called a security plan) or parts thereof, such as the ISO/IEC 17799 (2005), ISO/IEC 13335:1-5 (1996; 1997; 1998; 2000; 2001) standards, and frameworks as in BITS with Swedish Emergency Management Agency (2006), NIST with Bowen et al (2007), SSE CCM (2003), the emerging COSO (2007), Zuccato (2005), and de Oliveira Alves et al (2005). Kajava et al (2006) together with Lempinen (2002) state that there is a need to not only consider the standards, but to also advance from a discussion on standards such as the ISO/IEC 17799 (2005) to a change in the culture or organizational values. This paper will discuss what senior management should own and spend time with regards to IT- and information security, i.e. the strategic elements of IT- and information security and what can be managed and coordinated by one or few members of senior management. It is highly unlikely that senior management will spend time in understanding and coordinating an entire security programme [Kajava et al., 2006].

Dhillon (2007) has made a model to describe security strategy levels, linking security strategy questions to business strategy questions. Dhillon (2007) and Wylder (2004), in addition to many other books on management of information security, also outline classes of security decisions (strategic, administrative/tactical and operative). Wylder (2004) and Leveque (2006) discuss what strategic information security is and the necessity for it to be integrated into the corporate strategy, business planning and IT strategy for all ongoing operations. Wylder (2004) further identifies the importance of training, values, culture and senior management ownership, involvement and knowledge in policy, crisis management, business continuity planning, monitoring and measurement regarding information security. Leveque (2006) also thoroughly describes an information security strategy planning methodology for building a security programme. Dhillon's model and, indeed, Wylder or Leveque fail to explain how the different elements of strategic IT- and information security are either related or fit together from an organizational perspective.

The model presented in sections 2 and 3 builds upon the work in [Kajava et al., 2006; Lempinen, 2002; Wylder, 2004] by setting the scope for the attention of the entire senior management with regards to the IT- and information security to being targeted towards only the strategic elements. In order to do this, strategic elements of IT- and information security must be defined. The term strategic means that these elements are used by senior management to steer an organization. *Strategic IT- and information security* is an integral part of the following three elements: *Business Continuity Plan*, *rules*, and *education, practice and awareness*. The *Business Continuity Plan* is a plan that replaces the business plan during a crisis situation to assist an organization in returning to a normalized situation. The *rules* are comprised of IT- and information security policies and organizational values, and the *education, practice and awareness* consists of training on the business continuity plan, security policies, and general security training in addition to an awareness programme for all members of an organization as well as specific security training for senior management.

Regarding integrating IT- and information security in the management of organizations, Anttila et al. (2004) discuss the fact that information security is an integral part of modern business management systems in order to create a competitive advantage, requiring close co-operation between security experts and business executives. They also describe a variety of management related issues taken from international standards that, taken together, help to build up a security programme. They state that it is extremely important to understand information security issues in the context of business processes and that information security management is fully analogous to the management of other important areas such as finance, quality, and business risks. They point out that it is very important for senior management to be interested and spend a great deal of time on IT- and information security and that the area requires the same attention as all other important areas of a business.

However, it is highly probable that will not happen [Kajava et al., 2006] if senior management has to be responsible for the whole information security programme. In the model, this issue is addressed by limiting the ownership to only the strategic elements of IT- and information security for all of senior management and having one or a few members of senior management to manage and coordinate the rest of the security programme. However, it should be remembered that senior management is always ultimately responsible for the entire security programme. The model builds upon the work of [Anttila et al., 2004] and shows how the strategic elements of IT-

and information security are related and may be integrated in the steering of an organization.

To assist senior management in understanding both the complexity and their need to own and take care of the strategic IT- and information security, it must be explained in a less abstract manner [Kajava et al., 2006] and, where possible, to relate it to something more familiar. It is also necessary to explain how the different elements of strategic IT- and information security are related and fit together from an organizational perspective.

In section 3 we describe the model that may be used to explain this to senior management (as well as to all other members of an organization and for training purposes) in a straight forward manner providing both perspective and describing how the strategic elements are related. The model draws on the limitation of the senior management's responsibility to the strategic elements of the IT- and information security, the integration of IT- and information security and business planning, existing standards, and organizational values and cultural change.

2. Methodology

The research which has resulted in the model to explain strategic IT- and information security has been carried out in seven different companies and authorities during a period of seven years. In each an action research approach has been utilized. Action research has been defined as *“a participatory, democratic process concerned with developing practical knowing in the pursuit of worthwhile human purposes, grounded in a participatory worldview which we believe is emerging at this historical moment. It seeks to bring together action and reflection, theory and practice, in participation with others, in the pursuit of practical solutions to issues of pressing concern to people, and more generally the flourishing of individual persons and their communities”* [Reason and Bradbury, 2001].

Characteristics of action research are that action researchers act in the studied situations, that action research involves two goals; a) solving the problem (the role of the consultant); and b) making a contribution to knowledge (the role of the researcher), that action research requires interaction and cooperation between researchers and the client personnel, and that action research can include all types of data gathering methods [Gummesson, 2000]. In this research the researcher has acted as an expert or consultant in the role of case leader being responsible for the cases that also have involved client personnel at the participating organizations.

The original development of the model started seven years ago during the development of the business plans for two different corporations. In this work, a model to describe how the strategic steering tools were related to each other was required. The result of this was a graphic model to describe the business plan and rules, which are normally part of the senior management's strategic steering tools.

The model to explain strategic IT- and information security has been developed during cases in an additional five organizations (both corporations and state agencies) throughout the last five years. The cases have concerned development, implementations or training regarding the strategic elements of IT- and information security. In the cases one part has been to explain to senior managers, IT managers and employees what strategic IT- and information security is and how the elements are related.

During the process to explain the IT- and information security policies, new aspects have been added to the original model used for the explanations regarding the business plan and rules. The new aspects concern the impact from organizational

values, business continuity planning and the necessity for training. Finally, all the pieces have been collated and the model described below has been tested and validated in the latest of the five cases.

This case involved creating from scratch a new business continuity plan including a maintenance process for a state agency up to the point of handing it over to the part of the organization that will continue to maintain and develop the plan. All the steps of development, implementation and training were included in the work. The work was conducted in close cooperation with about 40 employees from all levels of the organization in excess of a one year timescale and run under the supervision of a senior management steering group. The work was divided into phases and at the end of each phase all deliverables were controlled and reflected upon, and adequate changes made according to the feedback from the reviewers (steering group and selected key employees). A final feedback addition was made to the business continuity plan and maintenance process after the training sessions of the crisis management teams using the business continuity plan to solve different scenarios where the organization's critical processes were affected. The whole organization also had a basic training session (where the model was used) regarding not only what business continuity planning is but also how the organization has been organized in order to handle any problems that arise.

2.1. Test results

To learn about the effects arising from the use of the model when explaining how the elements of strategic IT- and information security are related, interviews were conducted with eight interviewees who had participated in the case where the model was tested. The model was rated on a scale from 1.00 (bad) to 10.00 (excellent) and, in addition comments were also sought. The outcome of the rating was an average of 7.00, with a median value of 7.50 but with a standard deviation of 3.02. As there was a significant standard deviation, information regarding the interviewees' professional backgrounds was noted and a check made to determine whether there was any difference between those interviewees whose background involved coming from the private sector before entering the public one as compared to those who only had experience of the public sector. Four interviewees had extensive experience from the private sector and four had only worked in the public sector. The comparison showed that those with a private sector background rated the model with an average of 9.25, median value of 9.50 and a standard deviation of 0.96, and those possessing only a public sector background rated the model with an average of 4.75, median value of 5.00 and a standard deviation of 2.63. It was quite obvious that the model appeared to be better for those with a private sector background. Further investigation into the reason for this apparent anomaly showed that the interviewees who only had a public sector background were not used to the terminology used in the model. Thus, a variation of the model was developed, which was better adapted with a slightly different terminology for the public sector. The model and its variant for the public sector are described in the next section.

3.A model for understanding strategic IT- and information security

Most organizations use a business plan as a tool for senior management in order to steer the organization in a desired direction towards success. In figure 2, the business plan consists of:

- a vision, or a very long term goal, which is used to set the organization's orientation to strive in a certain direction
- objectives or part objectives, which are used to set planning targets to be achieved
- present situation, where the organization is at the moment
- a strategy, a plan regarding how to go from the present situation or position in order to achieve the objectives

The *business continuity plan* is an integrated part of the business plan which temporarily replaces the ordinary business plan when the organization is close to or has entered into a crisis situation. The purpose of the business continuity plan is to assist the organization in returning to a normalized situation. The business continuity plan is, in addition to the business plan, to be updated continuously, and not to become a discrete item to be left on a shelf and revisited every third year.

In figure 2, there is an oval where the strategy arrow moves from a normal situation (business plan) and enters into a crisis situation (business continuity plan). The crisis situation is the gray area in figure 2. Then the scenario changes and the senior management or the crisis management swaps from the business plan to the business continuity plan as quickly as possible in order to steer the organization back to a normalized situation (business plan).

The rules comprise IT- and information security policies and also the organizational values that set the boundaries for the members of the organization regarding what to do or not to do while using the organization's IT- and information resources. The rules are used to guide the members of the organization regarding how to behave inside the organization as well as towards others outside of the organization. The rules are affected by laws and regulations, what happens in society and ethics. Customers, prospective customers, business partners or user requirements regarding an organization's security are included via the "Externals", which affects the IT- and information security policies. The "values", complementing the policies, fall within the "in-house code of conduct" and can be written or unwritten – however they can be equally strong as they have been developed from the initial outset of the organization.

The *education, practice and awareness* includes IT- and information security training on the business continuity plan, security policies, and general security training and an awareness programme for all members of an organization as well as specific security training for senior management. Without the security training, there will be either no one or only a few members within an organization who will know how to act during normal situations as well as during a crisis situation.

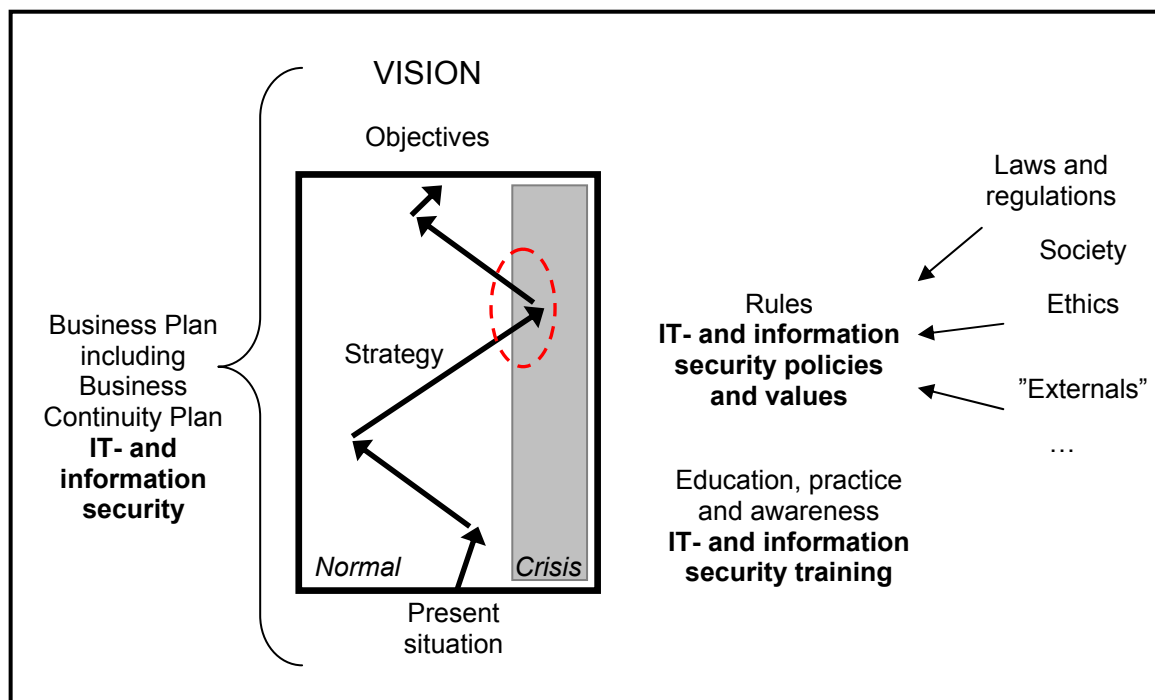


Figure 2. Model to explain strategic IT- and information security.

To summarize, the strategic elements of IT- and information security are *the business continuity plan*, which is an integrated part of the business plan, *the rules and education, practice and awareness*. These three elements are related to each other as they synergistically support each other.

To adapt the model for use in the public sector, the following minor changes were made regarding the terminology:

- Business Plan ⇒ Organizational Plan
- Vision ⇒ Assignment
- Strategy ⇒ Strategy/activities
- Present situation ⇒ Start

3.1. Comparisons between the model, standards and literature

A comparison of the model with the standards and frameworks used for the work with security programmes shows that the NIST and ISO/IEC 17799 have significant widths, but could be considered more as guides or checklists and do not directly screen out what is of strategic importance and how to explain these matters to senior management.

If looking more specifically at the strategic elements of IT- and information security, the business continuity planning standards and frameworks are mainly in the form of checklists and do not show where and how these might fit into the management of an organization and its business planning. Additionally, they do not state the reason why this might be considered important or be a concern for senior management. Wylder (2004) states that business continuity planning requires senior management involvement and understanding, and that it should be integrated with the business planning. With reference to the rules, Kolkowska (2005) and Hofstede

(1990) discuss the values involved whereas the model in this paper builds on the requirement for organizational values within strategic IT- and information security. It is also noted that regarding the security policies the standards and frameworks are mainly checklists. Wylder (2004) and Leveque (2006) state that bringing in information security into the organizational values and culture is the key to strategic information security. Regarding education, practice and awareness Anttila et al. (2004) and Wylder (2004) state that the strategic parts of IT- and information security are as important as the other topics within the management remit, and Kajava et al. (2006) and Wylder (2004) state that there is a necessity for increased awareness and understanding from senior management. Kajava et al. (2006), Lempinen (2002) and Wylder (2004) state that one member of senior management must participate and own the strategic parts of IT- and information security, and that commitment and participation from senior management in security trainings are required. To conclude the comparison, the model provides, in a simple manner, a perspective with regards to what is involved within strategic IT- and information security as well as how the elements are related to each other.

4. Further use of the model

The model is used to explain strategic IT- and information security to senior management – but it may also be used to explain this matter to all members of organizations during, for instance, training on IT- and information security policies or Business Continuity Planning. It is important that the entire organization from top to bottom has the same understanding regarding the strategic IT- and information security. This is important not only for maintaining the security level, but also because many members of an organization may be involved in solving problems during a crisis situation. During such a crisis situation, problem solving is required to be performed in as calm and systematic manner as possible - which requires a well trained organization with a uniform understanding of strategic IT- and information security.

5. Discussion on senior management responsibilities regarding strategic IT- and information in security programs

The strategic elements of IT- and information security, which were defined in the introduction, may be graphically described as is shown below in figure 3. As mentioned in the introduction, these are matters that the senior management should own and spend time on as they pertain to the strategic steering of the business.

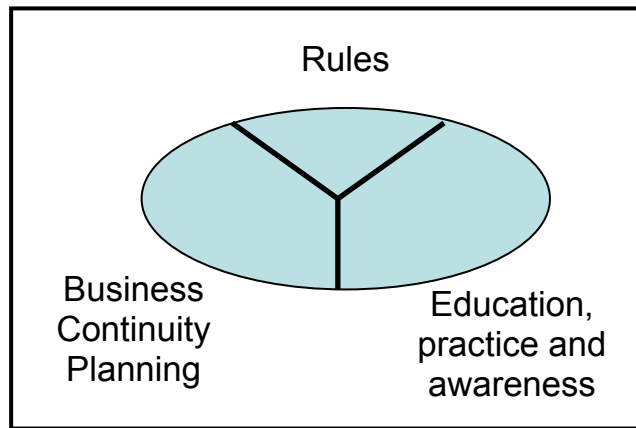


Figure 3. Strategic elements of IT- and information security.

As the importance of IT- and information security is increasing for most organizations, the strategic parts must be integrated into the senior management agenda on a continuous basis in order to provide for their care and maintenance [Anttila et al., 2004; Wylder, 2004; Leveque, 2006]. As senior management is always ultimately responsible for the IT- and information security (by law in most countries) they must ensure that the entire organizational security programme is maintained at an adequate level and properly cared for (i.e. due diligence and due care). However, the entire senior management usually has neither the time nor interest in coordinating the whole security programme [Kajava et al., 2006] – thus that which does not form part of the strategic elements may preferably be managed and coordinated by one or a few members of the senior management. It is highly unlikely that the entire senior management will spend sufficient time and effort to understand and coordinate a whole security programme [Kajava et al., 2006]. Figure 4 shows that the senior management should own and care for the top slice which consists of the strategic elements of the IT- and information security programme, and leave the remainder including the formation of a strategic plan for the security programme for coordination by one or a few members of the senior management and staff.

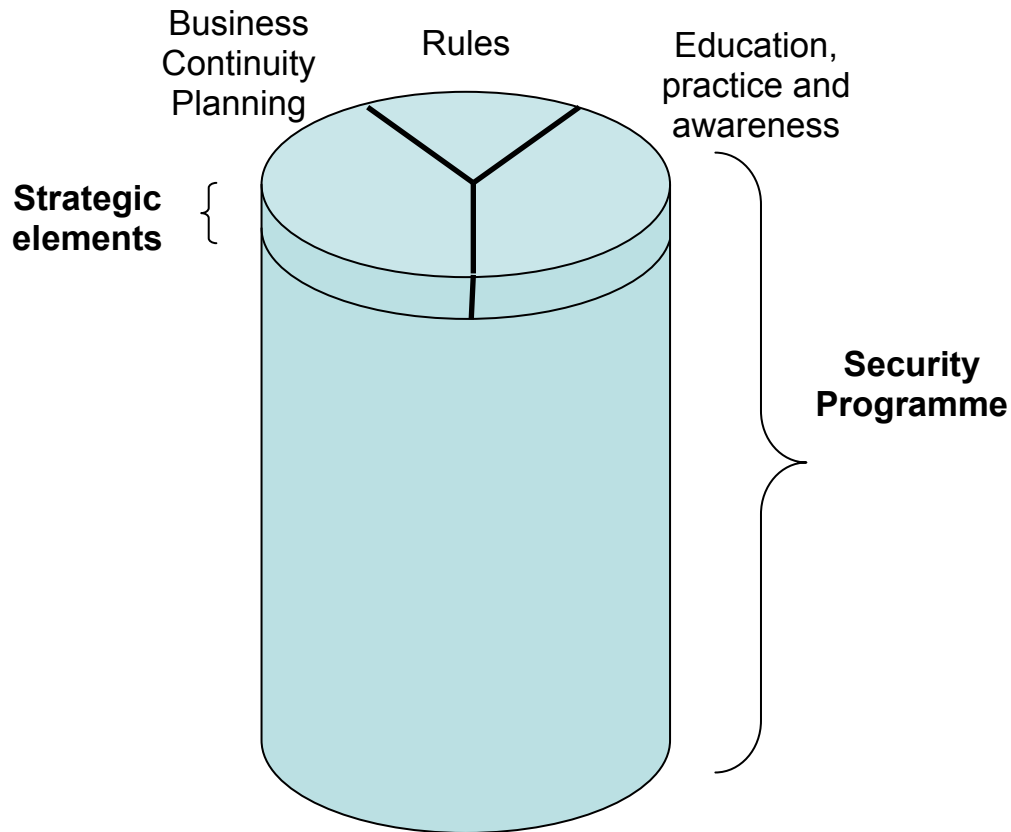


Figure 4. Security programme including the strategic elements of IT- and information security.

To clarify further, senior management should own and care for projects or activities involving the elements relating to strategic IT- and information security. However, this does not necessarily mean that senior management should perform all the work regarding these projects or activities as, for instance, the development or maintenance of a business continuity plan involves rather extensive tasks. Senior management should lead, participate and support the projects or activities.

6. Summary and future work

The model and the ideas presented in this paper are based on work conducted in five cases during the last five years. The strategic elements of IT- and information security have been defined and a model used to explain what strategic IT- and information security is to senior managements (top management) has been presented. The model was tested and confirmed during the last case and a variation of the model was made by changing some of the terminology to improve the result when using it in public sector organizations. The model may also be used to explain what strategic IT- and information security is to all personnel during training sessions.

We have also argued that senior management should own and care for the strategic elements of the organization's IT- and information security programme, and leave the operational levels to be coordinated by one or a few members of the senior management.

Interesting topics for future research are testing the described model further in different types of organizations, methodology for business continuity planning, and security training as well as IT- and information security policy problems.

7. Acknowledgements

We would like to thank Anders Lundkvist, CEO of the Arctic Group AB, and PhD Sören Samuelsson, Luleå University of Technology, for their valuable input.

References

- Anttila J., Kajava J., and Varonen R. 2004. *Balanced Integration of Information Security into Business Management*, proceedings of the 30th EUROMICRO'04, IEEE
- Bowen P., Chew E., and Hash J. 2007. *Information Security Guideline for Government Executives*, NISTIR 7359, NIST January
- COSO (2007), www.coso.org
- de Oliveira Alves G. A., da Costa Carmo L. F. R., and De Almeida A. C. R. D. 2006. *Enterprise Security Governance; A practical guide to implement and control Information Security Governance*, proceedings of the The First IEEE/IFIP International Workshop on Business-Driven IT Management, IEEE
- Dhillon G. 2007. *Principles of information systems security : text and cases*, John Wiley & Sons, NJ, pp112-121
- Gummesson E. 2000. *Qualitative Methods in Management Research*, 2nd Ed., Sage, Thousand Oaks, MA
- Harris S. 2003. *All-in-one CISSP certification exam guide, second edition*, McGraw-Hill/Osborne Media, pp20-21
- Hofstede G. 1990. *Measuring Organizational Cultures. A Qualitative and Quantitative Study across Twenty Cases*, Administrative Science Quarterly, 35, 2, pp286-316
- Kajava J., Varonen R., Anttila J., Savola R., and Röning J. 2006. *Senior Executives Commitment to Information Security – from Motivation to Responsibility*, proceedings of the International Conference on Computational Intelligence and Security, IEEE
- Kolkowska E. 2005. *Value Sensitive Approach to IS security – a socio-organizational perspective*, proceedings of the Eleventh Americas Conference on Information Systems
- Lam W. 2002. *Ensuring Business Continuity*, IT Pro IEEE, May June Edition
- Lempinen H. 2002. Security Model as a Part of the Strategy of a Private Hospital (in Finnish), University of Oulu, Finland
- Leveque V. 2006. *Information Security – A Strategic Approach*, John Wiley & Sons, pp3-20, 149-152, 175
- Grimaila M. R. 2004. *Maximizing Business Information Security's Educational Value*, IEEE Security and Privacy
- ISO/IEC 13335-1. 1996. *Information technology – Guidelines for the management of IT-security – Part 1: Concepts and models for IT Security*
- ISO/IEC 13335-2. 1997. *Information technology – Guidelines for the management of IT-security – Part 2: Managing and planning IT Security*
- ISO/IEC 13335-3. 1998. *Information technology – Guidelines for the management of IT-security – Part 3: Techniques for the management of IT Security*
- ISO/IEC 13335-4. 2000. *Information technology – Guidelines for the management of IT-security – Part 4: Selection of safeguards*
- ISO/IEC 13335-5. 2001. *Information technology – Guidelines for the management of IT-security – Part 5: Management guidance on network security*

- ISO/IEC 17799. 2005. *Information Technology – Security Techniques – Code of Practice for Information Security Management*
- Reason P., and Bradbury H. 2001. (Eds.). *Handbook of action research: Participative inquiry and practice*, London, Sage Publications
- SSE-CMM. 2003. *Systems Security Engineering Capability Maturity Model*. SSE-CMM Project, v 3.0 edition
- Swanson M., Wohl A., Pope L., Gance T., Hash J., and Thomas R. 2002. *NIST Special Publication 800-34 “Contingency Planning Guide for Information Technology Systems”*, June
- Swedish Emergency Management Agency (2006), *BITS – Basic Level for Information Security*, http://www.krisberedskapsmyndigheten.se/templates/Publication_1143.aspx, 2006:1
- The Swedish Finance Inspection. 2005. *Status of the finance industry’s crisis management 2005:3, report from 17-March-2005 (in Swedish)*, Dnr 05-1249-601
- Wylder J. 2004. *Strategic Information Security*, Auerbach/CRC Press LLC, pp1-16, 139-153
- Zuccato A. 2005. *Holistic Information Security Management Framework for electronic commerce*, Doctoral thesis, ISBN 91-85335-63-0