Information Security and Business Continuity in SMEs

Antti Tuomisto[1] and Mikko Savela[1]

[1] Laboris, Department of Information Technology, University of Turku, Finland

Abstract. The information society leads the way to the tomorrow's success. However, many SMEs are not on the fast lane of this highway. In this paper we give a description of what is going on and what is going to happen to SMEs in which the ICT has not yet established a central role. The aim is to describe the situation in these SMEs. The objectives of information society strategies might seem inappropriate or impractical from the perspective of non-IT-intensive SMEs. We describe the current situation of information security, and the development trends based on our survey. Our act-oriented framework suggests improvement areas in SMEs for information security and business continuity management. This management contains i) prevention, ii) recovery and iii) the procedure of information security initiation activities. The initiation process of new employees seems to be one of the few practical and cost-effective ways to make a durable change in the work place.

1 Introduction

All companies including SMEs use more and more information and ICT. This is in line with the information society strategies, see e.g. [4]. However, it is not clear what SMEs should do with IT related risks. Many SMEs business does not require any special ICT solutions. Current IT security guidelines are suitable for large corporations and IT-dependent businesses. However, we are concerned about the fact, that not all business lines are information intensive. The movement towards information society is strongly present. If this is the case, then what non-ICT-intensive SMEs should do about the information security and business security issues related to the ICT in their company? We know that high quality information is very dependent on the human actors. Also we have noticed that many studies on information security are biased towards information and communication intensive businesses and large organizations. This is argued because the volume of material and required technological knowledge, e.g. [7], are way beyond the resources and interests of many non-ICT-intensive SMEs.

We constructed a framework to clarify the non-IT-intensive business environment. We i) describe the current business situation of the traditional information security situation, ii) tensions of business continuity and upcoming technological visions/investments of the near future, and iii) the knowledge and actions of the workers. We emphasize the first two levels. The third level justifies the concepts and approach.

Tuomisto A. and Savela M. (2006).
Information Security and Business Continuity in SMEs.
In *Proceedings of the 4th International Workshop on Security in Information Systems*, pages 80-90

We conducted a survey to non-ICT-intensive SMEs based on the framework in order to deepen our understanding of the situation. Finally, we will derive preliminary guidelines for practical prevention and recovery actions to ensure information and corporation security for business continuity in non-ICT-intensive businesses.

The conceptual basis of this study is purposeful action in business organization. It requires understanding of the activities and the actors. We construct a general conceptualization for grasping the key features of critical knowledge and information of different types of companies. The concepts are built on the act-orientation, humanistic approach and inseparability [3], [13]. The work context includes not only the actor alone in her daily activities, but also other co-actors and other parties related to the production of the products and services. These include e.g. management, organizational support activities, sub-contractors, and authorities, not to forget the customers. In this study we analyze these at company level without entering the individual level.

First we study the current situation of best practice information security practices in SMEs in Western Finland. We get first hand data of how the traditional information security and business security is comprehended, and what it means to a company and its overall security needs. Next, we clarify the changing environment of globalization, networking, digitalizing, etc. business world, and how these are confronted at SMEs.

Finally, the business activities that are inseparable part of work activities performed by skilful people are examined. This act-orientation view is where the information and knowledge work including security issues related to business continuity actually take place. The everyday work of providing products or services, or other auxiliary activities are of key interest at this phase. The work related information (creation, storing, transmitting, use etc.) is studied. We attempt to clarify how these relate to current information security concepts, upcoming ICT trends and ensuring business continuity?

The main findings reveal the current status of traditional information security and corporation security. Also conceptions of the trends affecting entrepreneurship in information society are classified, and their meaning to the business is studied. Finally, the actors on the work scene are analyzed, and this fulfils our interpretation of the high quality information security and business continuity.

2 Act-oriented Framework of Information Security and Business Continuity

Information security is familiar to some extent to all entrepreneurs. The commonly used techniques (firewalls etc.) are widely spread, but too often the studies of the use of these techniques are biased towards information intensive companies. The SMEs differ from each other quite a lot and it is difficult to state anything valid guidelines for all types of SMEs. Number of employees, company history, maturity of used ICT, and information intensiveness are examples of variables that affect the role of current IT usage and traditional information security needs. Further, we want to try to see how the overall SME field, independently of the business line, uses these and how they see the effects of general technological development.

However, at the same time the global information society trend that is boosted with several governmental actions leaves no room for interpretations. Government, ministries, local administrations, chamber of commerce etc. have a significant impact on the current and forthcoming role of ICT in all aspects of life. Therefore, we included views from the current national-oriented information society and entrepreneurship literature (e.g. [4], [6], [9], [10], [11]). One conclusion is that technical infrastructure is believed to be adequate enough to provide means for efficient, high quality processes and interactions between all stakeholders (companies, customers, subcontractors, legislation, suppliers, employees, etc. worldwide). This in some sense means that a part of SMEs will disappear and new, information intensive and high education requiring businesses emerge (e.g. [8], [12], [16]). Still, before these scenarios and related utopia (or dystopia), we need to understand more deeply the connections between high quality information, its creation and processing. And we need to connect these to the information security as a natural part of business continuity of SMEs in order to find out what the overall change process is about. Key question is to find out what security activities are worth of investment in different types of SMEs in their journey to information society as a part of infostructure as Snyder [6] calls it.

Our objective is to form a picture of the current level of traditional technical biased information security in Finnish SMEs from one region and compare it to other studies, to seek out their comprehension of ICT trends in relation to their business in order to classify the expectations related to IT itself and their business and the business line in general. Empirical data is gathered with a questionnaire. Finally some thoughts are gathered upon the company's perception of management of information (data) and the activities that are related to the creation and use of the valuable organizational business information by employees (or other relevant actors).

We have two views on business: 1) ensuring the core business performance (continuity from employees and their knowledge and performance and high quality outcome) and 2) appropriate level of securing activities from misusages and damages. In traditional setting the latter is at least partly quite robust concept of required information security activities in medium or large organizations. These governmental of commercial guidelines try to cover all organizational areas. Yet, they are at their best in large organizations. Due to lack of resources and special knowledge of the various areas of information security issues, micro, small and medium-sized companies have different operational situations from which they reflect the need for information security and business continuity assurance activities. We are aware that e.g. in Finland at the moment there are many attempts to fill this knowledge gap. But based on our experience it easily happens that the information security and IT are separated from the actors and activities. This would lead to impractical and unrealistic solutions which do not help the SME to improve its securing activities and business continuity.

At the same time the business environment is changing, and globalization, networking, mobility etc. take place ([1], [2], [4], [5], [17], [18]). Thus, our first view above refers to the fact that all businesses face the situation where the amount and the role of information and knowledge increase. And thus the roles of the actors on the scene increase. How different types of companies position themselves and their activities that relate to ensuring business continuity at current situation? The actor-oriented view [3] demands us to try to find out where the high quality information is created, how it is used and stored, and by whom. A provocative argument for this is

that if the company does not hold any high quality information, then they do not have any serious need to secure it from misuse or damage. This is why we need to make an interpretation where the actors and daily activities are involved as an inseparable part of information security and business security.

Our framework has three levels and two phases of comprehension: interpretation of the current situation and construction of the act-orientated view on sustainable information security (see Table 1). The act-orientation is the basis, which can be applied to any (work) activity. But before the work itself is addressed, we describe the blurry picture of non-ICT-intensive SMEs comprehension of their current information security and visions of the near future (IT investments and development of the business).

Table 1. Framework for information security and business continuity analysis.

↑ Current and future business and security views towards actors	c) Information and knowledge (creation, modification, storing, (mis)use, etc.). The essence of skilful human actors in work context.	New actors on the (new) scene: information security and business continuity initiation ↓
	b) Conception of current and forthcoming info-structure; changes in e.g. information intensiveness and information work; IT and other investments.	
	a) Traditional information security and its relationship to enterprise security issues and ICT development.	

First, a) the traditional information security. Our framework starts from the basic concepts of current IT security studies. We attempt to create a well-analyzed interpretation of the SMEs current comprehension of relevant ICT security and business security. We want to get information of how familiar basic information security and related issues are, and what is the relationship of ICT and business at the moment in each company. This section focuses on information security events occurred during last few years. Also, the current status of IT is studied. The respondents' attitudes to security issues and their relationship to business continuity are studied.

Next, b) the large variety of security activities are reflected by the respondents. The business environment is addressed in the questionnaire. The relationship between business critical information and security issues are studied. This is the first suggestion of the locus of high quality data by relevant actors in business. How these affect to the SMEs view of their entrepreneurship and forthcoming (IT) investments? We study also the awareness of ICT related trends. The governmental information society strategies, company level actions and other research and development endeavors (either ICT or business line in question) have undoubtedly presented scenarios of future business in general or in a specific business area. These should have been noticed by now so that SMEs would be capable of commenting their current pressures for change. Do the workers in the near future tend to form a special group of actors, or do these embed to the overall business where such separation is not needed, or it is even considered harmful?

Finally, level c), where the locus of high (or poor) quality information is confronted. In this paper this is not fully studied. This level is about the actual business: what is the knowledge that keeps the business going? Are there any persons in company who are assigned to or concerned for security issues for the sake of business continuity? These give us a general picture of the business and information work in question, which will be addressed more in forthcoming studies.

3 The Survey

The primary research method for this study was a descriptive data from qualitative postal survey. A survey was chosen as the main data collection method because this research investigates the whole sector of SMEs. We try to describe the heterogenic target population of SMEs, and the inferred ideas of fundamental properties for high quality information and its management as a natural part of one's business.

The selected SMEs are SMEs between 1-499 employees on the Western Finland region. The data collection was designed in the form of a postal questionnaire. The questionnaire was addressed to person responsible for the information security and business security issues in the company (CEO or IT manager depending on the size of the company). Postal addresses were randomly selected from the database of Statistics Finland by the institution itself.

The sample included all sorts of companies between 1 and 499 employees. Based on our knowledge, a similar non-exclusive postal questionnaire to all types and sizes of SMEs has not been reported. We did not exclude IT branch, because the vast majority of companies are not in the IT field, only 3,6 % from the selected population was in the IT category (K72 in the Statistics Finland categorization). The survey itself included one IT representative, but they did not answer to the questionnaire. Thus, the survey was as planned, towards the non-ICT-intensive, "common" SMEs.

However, the micro enterprises (size 1-9) response rate was anticipated problematic. We decided to focus on the service sector and the secondary production entrepreneurs. We excluded farmers with no employees, charitable associations, sports clubs, housing corporations and non-profit associations and foundations. This reduced the number of companies from 25060 to 14129 companies. A test survey of four companies was undertaken in order to validate the questions and questionnaire. Based on the results on these experiences, we proceeded to the next phase.

Total of 701 companies were selected to the survey. Companies were divided in to groups shown in table 2. In table 2 the company size categories are used only for statistical purposes to solve the biased distribution of company sizes. Response rate between 10-20 % was expected. In order to get information from many size categories, we divided the micro companies into additional categories. To ensure that we get at least some data from different size of companies we made these additional categories.

Before conducting the survey we expected to get only few responses for the category of one employee. As shown in Table 2 we have not received enough responses from these to make any conclusions. We suggest that this category should have an approach of its own. However, we wanted to see these as a natural, and maybe a very

important part of the forthcoming information intensive society. The overall response rate was 19,3 % excluding the 1 sized enterprises. The response rate would be 16,4 % with the size of 1 enterprises.

Table 2. The survey population and the sample.

No of Emps	SMEs in the region (total 14129)	Sent Surveys (total 701)	Response rate
1	7315	120	3 %
2-4	4066	100	18 %
5-9	1379	100	16 %
10-19	737	100	16 %
20-49	418	100	24 %
50-99	133	100	20 %

The demographic results of the survey are not presented in this study. Rather, we will derive the main observations of the results based on our framework and build upon these a set of preliminary guidelines for practical information security and business security for SMEs.

The questionnaire was supported by company interviews. We planned 5 to 10 companies to be interviewed. Due to scarce resource of time (especially of SMEs), only two companies participated in an interview in which the business, technology and work processes were discussed in a more detail. These companies were voluntary respondents marked in the questionnaire. One is size of 50-99 employees, and the other is size of 100-249 employees. They are manufacturing and subcontracting companies. The survey suggested that the medium-sized companies would be beneficial objects for interview due to their organizational and technical history. Further, this size of companies must have undertaken some traditional information security and corporate security operations. The discussions supported our thoughts of the general situation, and next we will summarize our findings.

4 Survey Findings

The results are structured according to our framework. First we conclude our findings of the traditional information security, which, as expected, are in line with many other surveys. Then the views of the respondents of the forthcoming business and ICT are collected. Finally, the interpretation of the humanistic approach of high quality data and knowledge work is presented. Also, we shortly discuss the implications of the results as we travel through the actors on the scene view, and we present the practical, yet preliminary guidelines for SMEs' effective information security and business security from business continuity perspective.

4.1 Traditional Information Security and Corporate Security

Currently information security is seen very technical. If fire wall and anti-virus programs are installed, then many companies believe that all's well. The information security rules are considered as non-critical especially in smaller companies. User passwords are used, but they are trusted more than appropriate making the way of work even too careless: it seems that (other) users are not considered as an internal threat in SMEs: one could forget to log off when leaving one's work place causing no additional threat. Other problems are usual maintenance problems (updating software, crash downs, training etc.). This is partly managed by the skilful IT workers and technical staff. Yet, this could be a problem itself, if the expertise of these persons does not fulfill the needs of the company. The business line knowledge may be of top quality, but knowledge of the current evolving technologies may be at least partially outdated due to scarce resources for IT support.

Email is critical to all companies nowadays, and many production systems are used via network. This trend suggest that although the ICT is seen as the key investment in continuing and developing one's business, the recovery plans and prevention activities are only partial. Especially the security and recovery of the production systems seems to be insufficient.

The phase also leads to a preliminary size category for the SMEs. Companies over 100 employees are considered IT-dependent organizations, where information security and business security must be according to the current standards. This is independent of the business branch. They have resources for skilled professionals to manage the company's information security. The next category is 20-99 employees. It seems that these companies have to work actively to establish effective easy to manage the changing situation, independently of the future directions of business in question. Thus they need practical and cost-efficient guidelines to support their business continuity efforts. The size 10-19 is kind of intermediate group, and needs more research. Some of these companies could be in the 20 to 99 category, and some in the 2-9 category. These companies are often entrepreneur-led, and the future visions vary a lot. Finally the 2-9 sized companies form a category. This and the intermediate group (10-19) can be potential beneficiaries of the guidelines, although the IT maturity can vary a lot. Thus, it would be more of the question of indirect effects of the general information society rather than the ICT investments of the company itself.

To summarize, we suggest that the current situation in SMEs is not yet critical. The quality and cost perspectives require that companies use their scarce resources wisely and to right targets. We claim that SMEs current state of information and corporate security needs some training of IT in business context in order to avoid inappropriate ways of work and inadequate technical systems. But training is not enough.

4.2 ICT Trends and Anticipations to Business Continuity

What is the relevance of ICT to one's business in the near future? It seems that ICT related education and training is included in every respondent's future plans. These can be e.g. general guides of security, governmental programs or line of business specific training. The problem seems to be how to get these realized into practice.

IT and security services are searched for in the near future especially in the companies of size of 20-100 employees. Smaller firms probably do not have need or money, and larger companies already buy these services. The bigger the company is, the more crucial is the ICT. And vice versa: the smaller the company is, the less important the information security and corporate security seems to be. Especially, if the line of business is not IT related or information intensive. This may have some effective implications to the upcoming information society plans.

One result of this is that a significant portion of the SMEs do not comprehend the information security issue as a real threat to the corporate security and business continuity. Many of the production systems are nowadays connected to computer networks, and more systems are added to the network all the time. Thus, the security problems of the network expand to production level too easily.

Information society is seen as a positive, realistic and necessary change. Trust to the IT field's impact on business is strong: all IT is good; it improves business almost in all forms. However, the available resources of the SMEs to manage beforehand the implications of this are often inadequate. The changes will take place, and many SMEs live with the situation.

The increase of email and spam is already a problem to some companies. Individual companies do not have very good capabilities to avoid this problem. One company already first reads all email and then they have to remember to check the mail filtered by spam program. Some customer mails have already been missed due to this. Also, there is an increasing risk of production system specialized viruses. We believe that it is only a matter of time when these are confronted.

This phase showed that the current situation might be better than imagined. If the trend continues, in the third phase there will be more ICT artifacts and probably less knowledge of the management of them. This is an important observation.

4.3 Business Continues and Evolves: High Quality Service and Products

Our strong comprehension of the SMEs is that the actual outcome of the company is produced by skilful actors on the work scene. The humanistic interpretation of high quality information requires that these human actors are included in the framework. The view of SMEs independently of the business line produced an interesting suggestion of improving the information security and business continuity.

Especially in high technology fields the IT field is taken as a promising way to do all sorts of activities. Therefore, the use of ICT is generally favored. At the same time all sorts of data, information and even knowledge is attempted to be collected, stored, manipulated and transferred. But the costs and profits of this are not so evident, nor are the related security issues. Work life is changing, but as one respondent (R1) put it: "There must a great change of attitude before all these [information and knowledge issues] can be used as planned" [15].Therefore, we suggest that the continuing development of information security and business continuity must be introduced to the SMEs gradually by following themes: 1) Analyzing current information security needs and creation of information loss and work discontinuity prevention plan that focuses on key business items and functions. 2) Updating and establishing recovery

plan that fits to the resources available and business line in question. 3) Putting these two into practice by the management of the SME and the initiation of new employees.

The first two items are quite general information security recommendations, yet only together they form a meaningful whole. Currently, we believe that these first two can be engaged quite easily by the SMEs and with relative low costs. The problem, however, is how to change the current way of work to a more secure one. According to our observations, the only way this can be done effectively in SMEs is by integrating the information security and business continuity issues into initiation phase. There are no extra resources to additional training, and even if there were, the result is not always permanent change in work practices, and still the new employees must be trained. This tactic could lead to improvement of the initiation process itself by strengthening the content towards actual work. Also, a more positive adaptation to the security issue by new or reassigned employees could be resulted. The information system as an inseparable part of one work and act-orientation helps to understand these changes, see [3], [14].

5 Conclusions and Future Work

How SMEs could allocate their scarce resources into information security and business security issues in a manner which keeps prevention and recovery activities in a balance from the business continuity perspective?

First, the company should make actions in order to decide what items they have that must be secured. To do this, they must be aware that recovery is always needed, whether or not there are some preventive plans. The recovery could be the key perspective to the problem, because it reminds that the workers (actors on the scene) must do something extra work to make customers satisfied. Thus, finding out the key information can be produced at least partly by the actual actors themselves: what data must be protected and secured so that high quality recovery is possible to make the business continue and keep the damage as small as possible. Similarly, the minimum level of securing business continuity can be inferred to these points of action. Securing of enterprise data has no use if the data itself is no good. Thus: only high quality data needs to be secured by exhaustive actions. Otherwise, we suggest, that the actors themselves need to be more conscious of the work practice they are undertaking and its security and continuity relations. Preventive actions by training, education and technical instruments are all useful, as long these are in line with the business and workers daily work practices.

This leads to the most final conclusion: to deal with the information and knowledge itself as a natural part of (new) employee. The information security and corporate security are seen here as the course of action performed by the members of the organization. In SMEs the workers might have a better holistic view on the overall business and the work itself (including risks in personnel etc.). This should be used in analyzing continuity risks and produce work-oriented view on the corporate security and business continuity that can be integrated to the initiation process of the new employees. This approach is economical and gives good starting point to a more permanent change in work practice.

Finally, we emphasize the importance of a recovery plan, and the testing of these scenarios in a way that ensures the functionality of the plan, and especially its implementation when something unexpected occurs. As far as we know, it will happen.

Future work is needed to validate the situation of the non-ICT-intensive enterprises and to establish and test the suggested methods. Also, a more detailed qualitative analysis of several SME types would produce useful information of the work activities and information and IT usage (direct and indirect). These would help to understand the life cycle of high quality information in SMEs sized enterprises.

Acknowledgements

This research project was supported by Regional Council of Southwest Finland (Varsinais-Suomen liitto, www.varsinais-suomi.fi). Also, warm thanks to Antti Havola and especially to Pia Berg for their contribution to the project.

References

1. Badrinath, R., Wignaraja, G.: Building business competitiveness. International trade forum, 2, p. (2004) 6-7
2. Elfring, T., Hulsink, W.: Networks in entrepreneurship: the case of high-technology firms. Small business economics, 21, (2003) 409-422
3. Eriksson, I., Nurminen, M.I.: Doing by Learning: Embedded Application Systems. Journal of Organizational Computing, 1(4), (1991) 323-339
4. EU ICT Report: Strengthening competitiveness through co-operation: European research in information and communication technologies, Bryssel (2004)
5. EU Manufacture group: Manufuture: A vision for 2020. Brussels (2004).
6. Finland in the Global Economy: Finland's competence, openness and renewability. http://www.vnk.fi/tiedostot/pdf/fi/90444.pdf (9.1.2006) (2004)
7. Finne, T.: A Decision Support System for Improving Information Security. TUCS Dissertations, No 8, Abo Akademi, Finalnd, March (1998)
8. Hautamäki, A., Lemola, T.: Suomi uuteen nousuun: Innovaatiot ja osaaminen huipputasolle. Helsinki: Sitra, Edita (in Finnish) (2004)
9. Himanen, P., (ed.): Globaali tietoyhteiskunta. Kehityssuuntia Piilaaksosta Singaporeen. Helsinki, Tekes (in Finnish) (2004a)
10. Himanen, P.,: Välittävä, kannustava ja luova Suomi. Teknologian arviointeja 18, Tulevaisuusvaliokunta, Eduskunta, Edita, Helsinki (in Finnish) (2004b)
11. Information Society Program of the Finnish Government: Tietoyhteiskuntaohjelma. Helsinki, Valtioneuvoston kanslia (in Finnish) (2004)
12. Lindroos, P., Pinkhasov, M.: Information society: the ICT challenge. The OECD Observer, 240/241 (2003) 27-29
13. Nurminen, M.I., Eriksson, I.: Information systems research: the 'infurgic' perspective. International Journal of Information Management, 19, (1999) 87-94
14. Nurminen, M.I., Forsman, U.: Reversed Quality Life Cycle Model. G.E. Bradley, H.W. Hendrick (eds.) Human Factors in Organizational Design and Management. North-Holland, Amsterdam, (1994) 393-398

15. Savela, M., Tuomisto, A.: About information security and business continuity in SMEs in Western Finland. Turku (to be published, in Finnish) (2006)
16. Snyder, D.: Five Meta-Trends Changing the World. The Futurist, July-August (2004) 22-27
17. Terziovski, M.: The relationship between networking practices and business excellence: a study of small to medium enterprises. Measuring business excellence, 7 (2003) 78-92
18. Uhlaner, L.M.: Trends in European research on entrepreneurship at the turn of the century. Small Business Economics, 21 (2003) 321-328