The Role of Information Systems Security: Towards a More Secure Environment

SEPPO SIRKEMAA & EEVA YLÄNEN
Pori Unit
Turku School of Economics
P. O. Box 170, FIN-28101 Pori
FINLAND

Abstract: - Information technology and networks have an increasingly important role in our life. It is clear that current lifestyle, level of productivity and service would not be possible without information systems. However, there are numerous risks and threads that can cause problems, harm and interruptions. This paper is about understanding the risks, and issues the importance of developing security in organization's information systems.

Key-Words: - information systems, security, thread, development

1 Introduction

The importance of security is increasing. In most organizations the role of the information systems are vital for operations. Therefore, unplanned interruptions are not welcome as they can impact production, sales and numerous other processes and procedures within the organization. The reliability and robustness of the information systems are critical issues in today's networked world [1].

The security of the information system needs to be addressed. This is a challenging task because there are so many different threads and risks that impact operations more or less severely. Security-related issues affect also the trustworthiness of the organization that in turn may affect business relations and future business opportunities. Data on customers, for example, may get into wrong hands. Because of the business implications it is clear that the role of management is important in security development [2].

Security is an organization specific phenomenon, which needs to be understood by all users throughout the company. This is clearly a key issue, following basic security procedures – even though they should be incomplete – is better than security instructions which are not understood by the users [3].

In this paper we look at the challenges of information systems security in small business environment. The empirical research displays current state of security and gives ideas on future development areas in pursuit of an increased security against the various threads.

2 Understanding information systems security

The role of information systems is important in companies and business transactions [1]. At the same time the popularity of Internet is rocketing, most companies are connected to the Internet or they take advantage of the Internet. For example, in spring 2005 94 % of all companies in Finland 94 % use the Internet [4].

It can be argued that companies depend on networks and connections. Therefore, it is vital to protect company's information system towards different risks and threads that this brings to operations. In order to do this the company needs to a) map the risks, and b) develop security procedures [5]. Let us look closer at these issues.

2.1 Mapping the risks

It is vital to map the risks and understand the consequences of different possible security threads [2]. Profound analysis of risks is needed; it is the basis of security development. This is a process that goes throughout the organization, and needs top management support [2]. It is important to notice, that security analysis should be done regularly as new risks emerge, and the relative importance of different processes in the organization change.

There are several risks that challenge information systems. The risks range from forces of nature like fire and earthquake into ones that are result of human action. Outside intruders and organization's own employees are examples of the latter type of risks. A considerable part of risks that thread information systems is result of human action. Human action, activities or behavior can be either unintentional or intentional. For example, an employee might send important memorandum to incorrect recipient, or IT-staff might forget to change a tape in the backup device. These are often unintentional actions, misunderstandings or simple mistakes. Instead, programming and spreading computer viruses is an intentionally "bad" activity where the goal may – for example - be to harm and damage the recipient of the virus program.

It is often argued that Internet is the main source of risks as it is not controlled by anyone [6]. Internet is the hideaway for hackers and intruders, who are ready to hack organizations connected to the global Internet. New ways to attack and damage are continuously being developed, and so there are many kinds of threads. Risks from the Internet can be divided into a) external attacks, b) intrusions and c) malicious software like viruses and worms. It is still important to notice that often security problems have their roots inside the company. [2]

External attacks try to harm operations in some way. One of the most common types of external attacks is DoS (Denial of Service). Massive amount of requests consume system resources so that server crashes or users are unable to use the system because of the massive network traffic generated by the attacker [6], [7]. The attack may also come from several addresses so that it is more difficult to locate and block the requests. This kind of attack is a DDos (Distributed Denial of Services).

The role of the human is critical in information systems security, and often the user is the weakest element in security-related issues [1]. The users should better know could happen if they do save their files to personal computers hard disk instead of the company's server, leave their computers open instead of logout when leaving the desk, use too simple passwords and write them to notepads etc. The list goes on and on, and illustrates that many security threads are result of users who act in an insecure way. Consequently, information on proper working procedures is needed.

The best way to avoid and minimize user-related risks is to increase general awareness in information systems security. Education and information on current security threads should be available. Even though there had been security campaigns, and arrangements for user advice, security issues need to be discussed periodically. In this way user's current knowledge can e maintained and more secure methods will be learned. Also for new employees must be taught, it would be a good idea to include security training as part of the welcoming procedures.

2.2 Developing information systems security procedures

Mapping different risks is the basis of security management. Not all risks and threads can be eliminated; they must be managed depending on their possible impact on operations [2]. Consequently, developing information systems security is based on [2]

- Robust information systems infrastructure that contains basic systems level security like user authentication firewalls etc.
- Security procedures which are straightforward and tight: for example backup procedures need to be followed accurately or otherwise there is no guarantee that important data is backed properly
- Security procedures which are well documented
- Procedures for crisis need to be planned and understood at all levels throughout the organization
- Security exercises reveal problems in existing security and make it possible to recover should a real disaster strike

One key issue in security development is understanding and commitment to security development at all organizational levels [2]. It is the task of the top management to set the strategy and targets information systems security. Putting the strategy into action is the task of others in the organization. Line managers, experts and key persons play an important part in the realization of the strategy.

Development of the information systems security is a continuous process. The processes and procedures in the organization must be such that they guarantee the integrity of data and information [6]. This is result of three kinds of control mechanisms: preventive, feedback and preventive feedforwarding controls. Preventive security aims to keep the system in operation by preventing unauthorized access, downtime and interruptions in operation. The other two mechanisms check current status and based on it alert or make adjustments so that an optimal system status could be achieved. [8]. Ideally, information systems security should be developed so that problems could be avoided and possible consequences minimized before something serious happens.

Development of a disaster recovery plan can help the organization in focusing to key areas and risks. It is a plan that is aimed to recovery from a possible disaster where important data has been lost. With this plan the organization may continue operations depending on the disaster. A disaster recovery plan makes it possible to avoid confusion and chaos as procedures, activities and roles of different individuals have been planned in advance. There might be different alternatives and plans to choose from, as in a crisis situation there is short of time for decent planning.

Properly implemented recovery plan guarantees that critical resources are better protected. Important data must be available and recoverable from backup devices. Without data on sales, orders etc. operations cannot continue, and so critical data must be mapped and backed properly. The disaster recovery plan makes also recovery faster than in a case where no a-priori planning has been done.

In this chapter we have emphasized the role of information systems security planning. It is still important to keep in mind the role of the user. Plans do not help much if users are unaware of them or act in a way that is unwise from security perspective. Understanding security and commitment to security plans on individual level is a key issue for corporate information systems security. As noticed by Wadlow [3] “A weak policy that is well distributed is better than a strong policy no one has read”.

3 Security in case organizations

In this part we explored security in selected case organizations. The case organizations operate in Satakunta region in western Finland. We were focusing on information systems security in different companies and other organizations that are located in this geographical area. The number of organizations is high, and so eliminated small organizations from the group of case organizations. Organizations with 25 employees or more were selected from all organizations (the official database of all organizations in the area is maintained by Satakunnan Yrittäjät, member of Suomen Yrittäjät Ry, http://www.yrittajat.fi). With this restriction 75 organizations were selected to the group of case companies (list is in appendix A).

Larger organizations we selected to the group of case organizations on purpose, it is assumed that information systems, information systems management and security related issues are better managed opposed to smaller organizations where these issues may not yet be organized. We believe that the results will reflect the current situation and challenges of security management also in smaller organizations as well.

The case organizations were studied with a questionnaire. We wanted to get answers from those persons who are responsible for information systems security in their organization. In a typical case the person who answered the questionnaire was CEO or IT manager. The questionnaire was based on questions used in following other surveys: Global Security Survey (2004) from Deloitte Touche, the 9th Security Survey from Computer Security Institute (CSI), Computer Crime and Security Survey (2004), E-Crime Watch Survey from CSO Magazine and CERT (2004) and Global Information Security Survey 2004 from Ernst & Young.

We approached the case organizations with email where the research area - information systems security – and goals of the study were explained. The email contained also a link to a web-form, which was the actual questionnaire. A month later another email was sent to the case organizations, now we kindly reminded them to answer the questionnaire. This was done in order to increase the number of answers, and also because we experienced some technical difficulties in the data gathering phase. The operator’s server crashed during our study, and this impacted the number of responses. The response rate was low, only 22,2 percent of the case organizations answered. Despite this the results reveal the need to further develop in information systems security in organizations in Satakunta region. It is not possible to generalize the results, or to draw drastic conclusions from the results.

In the analysis phase we used the number of employees in interpreting the results. Secondly, the turnover of the company was used in analyzing the results. From this perspective the group of case organizations is heterogeneous, there where both small companies (yearly turnover less than 5 MEUR) and large companies (over 15 MEUR). The turnover was rather evenly spread in the case organizations, which allows us to study the results in more detail. There is a clear connection between the number of employees and turnover: when the turnover increases the company employs more people (Table 1).

Most of the case companies operate in manufacturing. There are one company from the logistics and services, and one form the IT-industry; all others are from the manufacturing industry.

The organization of the information systems management interested us. Especially we looked at how the development takes place, and what is the role of outside experts, systems providers, tele-operators etc. in the security development. It was found that most organizations involve take advantage of their partners in development. Shortly, advice and expertise are needed in the development process.

Up-to-date information on security, security regulations and advice can be found on the site maintained by the Finnish Communication and Regulatory Authority (FICORA). This organization promotes the development of information society in Finland. FICORA issues technical regulations and coordinates standardization work at national level. It supervises the technical functioning and security of communications networks, as well as ensuring fair competition among different operators in the country. One important group in FICORA is the CERT-FI task force, which focuses on preventing and controlling the violations of and threats to the data in information systems. The questionnaire revealed that most respondents were unaware of the information and services provided by FICORA. Clearly, FICORA needs to market it's services so that more companies could take advantage of the security related information and advice in developing their security.

In most case organizations top management recognizes the importance of information systems security. Only in three cases top management considers information systems security as a critical issue. In one case organization information systems security is not seen as very important area. It is worth noticing, that in all case organizations was security seen important, whether it is critical or not is a matter of degree.

Responsibilities in information systems security are somewhat unclear. In some companies there is a person who is responsible for information systems security, but in other case companies this is not the case. However, our question was set in a way that it is not clear whether there is a person who is responsible for security. The answers may also indicate that the person who answered the question is unsure whether the task has specifically been assigned to someone in the company. If this is the case, responsibilities are unclear.

The next question studies whether there is information on security related procedures in the company. In this question, and in several others, we used a modified Likert-scale in capturing information on security issues. The respondent had also a don't know -option if the person answering would not like to reveal his or her opinion, for example. The results indicate that in larger organizations it is typical to inform employees on security related issues. However, in smaller organizations this is not the case as most respondents seem to see that there is not available information on security procedures (Table 2).

Similarly, we asked how regularly are security procedures tested, verified or updated (Table 3). The results show that there are no clear answers to this question, and the size of the company does not seem to affect checking of security procedures. One possible interpretation to the situation is that the respondents may be aware of security procedures, but the procedures may not be regularly verified or updated. Verification of security related procedures can be part of regular development procedures, but it may be forgotten or left out when other critical issues emerge.

Information on security is a key issue. We continued by asking about whether there is training on security issues. As seen in table 4 there is not enough security related training in case organizations. The answers are spread, and the size of the company does not seem to affect whether there is training on security issues. Even in largest organizations the availability of security training is inadequate. Consequently, security training needs to be developed in all organizations. The situation is not disastrous as users are otherwise being informed on organization's security practices. This takes place in the introduction and welcoming procedures when the employee enters the organization, for example. When we discussed further it became apparent that information on security issues tends to be unplanned or scattered. Security issues should be packaged in a way that all vital information and practices are covered. It would also be useful if the user could find the information later.

Based on this study are different security threads well identified in the case organizations (Table 5). Only two smaller companies disagree indicating that they do not know security threads well. We asked further whether the organizations information system is guarded against these threads (Table 6). The idea was to find out how different threads have been identified and whether there are procedures that eliminate each thread. These security procedures include user authentication, frequent password changes, virus scanners, firewalls etc. Even thought most answers agree meaning that the information system is guarded against identified threads there is more dispersion in the answers when compared to the previous question. In fact, almost half of all answers fall into disagree, strongly disagree and don't know area. These results reveal that almost in half of the cases the information system is not guarded thoroughly. This is an important notion requiring immediate action in the case organizations.

It was found out that organizations are better prepared to threads from the outside than internal security risks. The results indicate this clearly (Tables 7 and 8). In largest companies planning and disaster recovery have been addresses, but not in all cases. Sadly, lack of disaster planning is a “de facto” -situation in most case organizations. The risks and threads from organizations own actions and employees are not seen as serious as external threads. An employee who does not understand the implications of missing data backup can be a critical risk, for example. Focus should be shifted from covering the outside border of the organization to management of internal risks.

4 Conclusion

The information systems security has become increasingly important in organizations. Connecting to the Internet has opened the doors for several kinds of threads. For example, viruses spread rapidly and can have tremendous impact on operations. Another type of risks is in employees who may be unaware of the consequences that are result of inappropriate security-related actions.

In general, it is not possible to develop a 100 % protection against all risks. However, analyzing the risks and developing a security-level which matches the risks can minimize the damage if something unwanted should happen. Based on this research different security threads are rather well known. However, almost half of the case companies did not have proper shields against these threads. Proper backup-procedures and recovery procedures are vital, otherwise operations cannot continue if unwanted issues should happen.

Empirical evidence indicates that organizations have identified different security threads. There is still work to be done. For example, action plans for disaster recovery need to be developed. Also regular verification of security issues is missing in most cases. The size of the organization does not seem to affect security management – in both smaller and larger organizations there are unmanaged areas in security.

Development of the security towards external threads is a vital issue. In addition, information on secure working procedures is needed so that internal threads could be minimized. In this research we found that while organizations have been developing information systems security it relates to external threads. It is clear that better management of internal threads is needed, for example security training and availability of security information should be better organized.

Security development and implementation covers a relatively long time [9]. Firstly, it takes some time before changes can be implemented. Secondly, new threads emerge as time goes on. This highlights the fact that development of security is a continuous process.

References:

[1] Napier, H. A. – Judd, P. J. – Rivers, O. N. – Wagner, S. W., *Creating a Winning E-Business.* Course Tech.: Canada, 2001.

[2] Applegate L. A. – Austin R. D. – McFarlan F. W., *Corporate Information Strategy and Management.* McGraw-Hill: Irwin, 2003.

[3] Wadlow, T. A., *The Process of Network Security: Designing and Managing a Safe Network.* Addison Wessley, 2000.

[4] *Statistics Finland 2005* <http://www.stat.fi>, retrieved 1.9.2005.

[5] Attaran, M. – VanLaar, I., Privacy and Security on the Internet: how to secure your personal information and company data. *Information Management & Computer Security*, 7/5, 1999.

[6] Laudon, K.C. – Laudon, J. P., *Management Information Systems : Managing the Digital Firm.* Upper Saddle River (NJ): Prentice Hall, 2002.

[7] Bidgoli, H., *Electronic Commerce, Principles and Practice.* Academic Press: California, 2002.

[8] Curtis, G. – Cobham, D., *Business Information Systems, Analysis, Design and Practice.* Prentice Hall: Harlow, 2004

[9] Purser, S., *A Practical Guide to Managing Information Security.* Artech House Inc.: Boston, 2004.

Tables

	Number of employees			
Turnover	Under 50	50 - 100	Over 100	Total
Over 15 MEUR	-	4	2	6
10 – 15 MEUR	-	2	1	3
5 – 10 MEUR	1	2	-	3
Under 5 MEUR	4	-	-	4
Total	5	6	3	16

Table 1. Turnover and number of employees in the case organizations

	Availability of information on security					
Turnover	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Don't know
Over 15 MEUR	-	100 %	-	-	-	-
10 – 15 MEUR	-	100 %	-	-	-	-
5 – 10 MEUR	-	100 %	-	-	-	-
Under 5 MEUR	25 %	-	25 %	50 %	-	-
Total	6 %	75 %	6 %	13 %	-	-

Table 2. Availability of information on security related procedures

	Security procedures are verified/updated periodically					
Turnover	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Don't know
Over 15 MEUR	17 %	33 %	33 %	17 %	-	-
10 – 15 MEUR	-	33 %	33 %	33 %	-	-
5 – 10 MEUR	33 %	33 %	33 %	-	-	-
Under 5 MEUR	-	25 %	25 %	25 %	25 %	-
Total	13 %	31 %	31 %	19 %	6 %	-

Table 3. Security procedures are verified/updated periodically

	Employees are trained on security issues					
Turnover	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Don't know
Over 15 MEUR	-	33 %	33 %	17 %	17 %	-
10 – 15 MEUR	-	-	-	100 %	-	-
5 – 10 MEUR	-	-	33 %	67 %	-	-
Under 5 MEUR	-	-	-	100 %	-	-
Total	-	13 %	19 %	63 %	6 %	-

Table 4. Employees are trained on security issues

	Security threads have been identified					
Turnover	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Don't know
Over 15 MEUR	33 %	50 %	17 %	-	-	-
10 – 15 MEUR	-	100 %	-	-	-	-
5 – 10 MEUR	-	67 %	33 %	-	-	-
Under 5 MEUR	-	50 %	-	50 %	-	-
Total	13 %	63 %	13 %	13 %	-	-

Table 5. Security threads have been identified

	Information system is guarded against identified threads					
Turnover	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Don't know
Over 15 MEUR	17 %	33 %	33 %	-	17 %	-
10 – 15 MEUR	-	67 %	-	-	-	33 %
5 – 10 MEUR	-	67 %	33 %	-	-	-
Under 5 MEUR	25 %	25 %	-	25 %	25 %	-
Total	13 %	44 %	19 %	6 %	13 %	6 %

Table 6. Information system is guarded against identified threads

	Organization is better prepared to threads from the outside than internal security risks					
Turnover	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Don't know
Over 15 MEUR	-	33 %	33 %	17 %	17 %	-
10 – 15 MEUR	-	-	-	100 %	-	-
5 – 10 MEUR	-	-	33 %	67 %	-	-
Under 5 MEUR	-	-	-	100 %	-	-
Total	-	13 %	19 %	63 %	6 %	-

Table 7. Organization is better prepared to threads from the outside than internal security risks

	My organization has an action plan in case of a disaster					
Turnover	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Don't know
Over 15 MEUR	-	50 %	17 %	17 %	17 %	-
10 – 15 MEUR	-	-	-	67 %	-	33 %
5 – 10 MEUR	-	67 %	-	33 %	-	-
Under 5 MEUR	-	-	-	50 %	50 %	-
Total	-	31 %	6 %	38 %	19 %	6 %

Table 8. My organization has an action plan in case of a disaster