Explaining Security Management Evolution through the Analysis of CIOs' Mental Models

Jose Maria Sarriegi, Jose Manuel Torres, Javier Santos

Tecnun - University of Navarra

Pº Manuel de Lardizabal 13, 20018 Donostia - San Sebastián, (Spain)

Phone: 34943219877 Fax: 34943311442

jmsarriegui@tecnun.es, jmtorres@tecnun.es, jsantos@tecnun.es

Abstract

Information Systems are a key factor for firms' competitiveness. Thus, their efficient management has become a key concern and security management one of the most relevant issues. An empirical study has been developed to determine the characteristics of security management within Small and Medium sized Enterprises (SMEs). A summary of the main data from this study is presented.

The results of this study have showed that the evolution of security management within firms has evolved through similar patterns of behaviour. Some phases have been defined to explain the evolution of security management within SMEs. The defined phases are: Growth, Integration, Formalization and Involvement. To explain these phases causal loop diagrams and behaviour over time graphs have been used. Both elements help to more accurately understand the mental models of the people in charge of managing the security of information systems.

KEYWORDS: Security, Information Systems, Mental Models

1 Introduction

Information is nowadays the main resource for any firm. Firms can only obtain competitive advantage through better decision making processes and that is why they need very accurate information systems (ISs). These last years firms have invested huge amounts of money in order to implement ISs.

If these ISs did not work properly, firms would have serious problems. Without them, a firm could at best survive a few days, at worst a few minutes. Hence, ISs availability has already become a key concern for almost all firms, even if they do not know exactly how to manage it.

Small and Medium sized Enterprises (SMEs) represent the vast majority of firms in the Basque Country, a traditionally industrial region between the north of Spain and the south of France (2.112.204 people; 7234 km^2; more information can be found in www.euskadi.net).

Within the majority of the SMEs the IS department is small, as they do not consider it a core competence. Not long ago, SMEs have begun dealing with IS management and most recently with security management and they yet have some difficulties to overcome. An empirical study has been developed in order to define the current situation.

The results of this study have showed that the evolution of security management within firms has evolved through similar patterns of behaviour. This can be explained by analysing the evolution of the mental models of their CIOs (The term CIO, Chief Information Officer, might be too ambitious for a person who manages a department

consisting of 2 to 10 people, but it is the term that will be used in the context of this paper to refer to the directors or those in charge of the IS department).

The role of the CIO is very relevant for SMEs security management, as they are the key people who determine the security culture of the firm. Eliciting their knowledge and perspectives about security can be very significant to help firms implement effective security management.

2 Management of Information systems

ISs have expanded into firms very significantly over the last few years. Consequently, their size and complexity have largely grown. This has caused the task of managing the firm's ISs to become critical, tough and intricate. The need of having suitable management mechanisms to ensure the effective deployment and utilisation of the implemented IS resources has been recognised by the researchers that have studied this issue (Ranganathan and Kannabiran, 2004).

Time constraints forces ISs to be implemented and used before their management tools are established. Likewise, these management tools are designed and built after the ISs are running. This happens even more often within SMEs, where the managerial actions are limited by the scarcity of technical and managerial personnel.

Current literature proposes a new approach to ISs management, claiming that ISs success is a function of management orientation and management processes rather than the simple application of technology itself. (Remenyi et al., 1999). The technical oriented background of the SME´s CIOs makes the development of a formal ISs management difficult, as they prefer to focus on technical aspects.

ISs security is usually included as a non functional requirement of the IS, together with efficiency, usability, correctness, flexibility and others (Mylopoulos et al., 1992). Non functional requirements are difficult to enforce during software development, to validate for the user once the system has been built up and to manage when the application is running.

Until recently, security did not seem to be a major concern for information system managers, neither for selecting the applications, nor afterwards (Brancheau et al., 1996). Security was not considered to be a relevant issue in deciding which ERP will be implemented into a business (Kumar et al, 2003).

This tendency is changing, and security is currently recognised as a main factor in the management of ISs. These last few years laws have been developed, there are many new security devices, specialised consultancies have flourished and innovative models and methodologies have appeared. All this facts prove the current relevance of security management.

3 Security Theory

Firms are very dependent on their ISs. If these systems do not work properly the losses can be significant. These losses include lost orders, decreases in productivity, damage to reputation and employee morale and others. Even if it is difficult to accurately measure all of these losses, there are some examples that could demonstrate that security has a great economic impact onto firms nowadays. The 2004 CSI/FBI survey estimates the total losses for their 269 respondents in more than 140.000.000 $ (Gordon et al., 2004).

ISs are complex entities for firms. They consist of interconnected application networks, including some of these: ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), PDM (Product Data Management), APS (Advanced Planning System), OLAP (OnLine Analytical Processing), Workflow applications, etc. They also are influenced by several operating systems, hardware platforms, servers, personal computers and other equipment. Therefore, the design and maintenance of all these elements is not an easy task.

Security is also a broad issue, including, at least, confidentiality, integrity and availability. It needs some technical controls (such as antiviruses, spam filters, firewalls, IDSs, Intrusion Detection Systems, Backup mechanisms and others), but also both formal and informal controls (Dhillon, 2001). Formal controls are the procedures, instructions and responsibilities explicitly designed for the correct use of technical security controls. Informal controls are related to security culture and commitment. These three kinds of controls (technical, formal and informal) must be in place to have a secure environment. The lack of any of them could generate a security breach (Torres et al., 2004).

Organizational issues, as with the loss of organizational memory and the lack of community mechanisms for monitoring changing threat environments, can be the primary cause in security failure (Anderson, 2001). Hence, moving from pure technical security towards managed security is a current requisite.

The "human side" of security is particularly relevant. It can be said that an organization's staff is the most cost-effective countermeasure against security violations (Rudolph et al., 2002). Bruce Schneier states that it does not matter neither how the network is protected nor the safety devices that have been settled, but the real significance lies in who is using and defending the system (Schneier, 2001). Thus, the importance of CIO's mental models is significant, as they are the most influential people in SMEs.

Not only CIOs' attitude is relevant, also users influence security. The users tend to relax security, as they feel more comfortable in non-restricted environments. Misperception of risk and superstitious learning are factors that lead people to erode the compliance of security norms (Gonzalez, 2003).

Security has some characteristics that could also be applied to the so-called non functional requirements:

- It is difficult to measure. There are not standard units for security. This causes that determining its returns is not possible.
- When it is working, is often invisible. A secure environment does not apparently differ from an insecure one. Its absence is much more recognizable than its presence.

There are several methodologies for managing security. The Corporate Information Security Working Group identified at least 81 different sets of BSPs, best security practices (Corporate Information Security Working Group, 2004). This means that SMEs can select which security model they would like to implement from a broad range.

Although there are some other security models, as CobiT (COBIT Online), which seems to have a significant implementation in American companies, the only one which is widely known in European companies is ISO 17799 (Certification Europe, 2004). This

internationally recognized information security standard identifies a range of controls needed to operate in a trusted environment. This information security standard proposes a common language for proper development of security policies from system development to business continuity.

It is organized into 10 major sections but according to the latest edition of the 17799 community portal (The ISO 17799 Service & Software Directory), the most important controls are: Compliance, Security Policy, Security Organization, Personnel Security and Business Continuity Plan.

Together with this ISO 17799 there is another guideline that indicates how to implement the selected best practices in the firm (UNE 71502). This Spanish norm includes the traditional PDCA (Plan, Do, Check, Act) cycle to implement the selected best security practices in the firm.

4 Security Practice

In order to analyze the actual practice of security management, we conducted an exploratory study of 20 Small and Medium Enterprise (SME) cases in the Basque Country. 10 firms were industrial, 3 research centres, 2 banks, 2 engineering services, 1 hospital, 1 broadcasting company and 1 public administration institution.

This work seeks to contrast theory and practice by analyzing the management carried out by Basque SME(s). We individually interviewed each firm, where we usually met the CIO. We also got in touch with two people who were explicitly designed as Security Directors, one of their multiple responsibilities. All the obtained information was compiled into a report, which was sent to every firm. We received the feedback from the firms through individual communication and in a meeting session that was organized for sharing the comments about the report.

Through this study, it was possible to analyze SMEs' security experiences, their current tools and management models, their achieved results and difficulties overcome. We were able to get a more realistic point of view and also valuable data to help Basque and international organizations interested in security management improvement.

In other words, this empirical study allowed us to characterize firms' security management evolution and therefore gain a widespread vision of their current situation and their future evolution. This section discusses general information about these firms but, does not fall into specific details about the collected data for confidentiality reasons.

4.1 SMEs Starting Point

The reasons that triggered Basque SMEs to focus on security management of ISs have slightly differed from case to case. These are the most significant starting points:

4.1.1 Internet Connection

Most of the interviewed companies highlight Internet connection (mid 1990) as one of the main landmarks that forced their interest for information systems security. The evolution of information systems along with the opening to Internet has supposed an important step for changing CIOs' way of thinking. Internet security related incidents published in newspapers, magazines and books have accelerated this process of awareness.

4.1.2 Data Protection or Other International Law Fulfillment

The Spanish Data Protection Law (LOPD), created in 1999, is changing the traditional way to operate, being another security management starting point. This law requires high confidentiality of personal data, forcing SMEs to document information related processes.

Companies which their headquarters are based internationally have to fulfil international laws. For example, interviewed companies that have their headquarters in United States must follow the American SOA (Sarbanes-Oxley Act) law. This means strict security protocols.

4.1.3 Security Incidents

Unfortunately, economic losses seem to be the fastest mechanisms to increase security awareness. Some organizations did not start implementing strict security procedures until they experienced information losses, denied of services, floods and daily activity breaks in. Some other companies have recurred to professional hackers in order to find vulnerabilities on the system and so, take corrective actions.

4.1.4 Connecting to External Information Systems (customers, suppliers, etc)

In some cases, commitment to security comes from new systems' connections to the outside; either company headquarters or employees that work outside the company like sales representatives. This system connectivity increases the system's complexity and therefore, the firms require proper security management.

4.1.5 New Information Systems and Architectures

The information system upgrade process, especially those based on ERP (Enterprise Resource Planning) systems, has supposed a change in the security policies. System security commitment has significantly increased since organizations have centralized their information in servers. According to SMEs, centralizing information allows them to ease data management, providing a better service to end-users. However, this centralization made them realize the importance of security management.

4.2 SMEs Security Management Culture

Although it was possible to find management styles located between these two extreme situations, firm's security culture varies between two opposed extremes:

4.2.1 Culture focused on supervision and control

The system openness is analyzed in each case and therefore, the company begins with very restrictive policies that can become more relaxed if necessary. Permission must be given to modify data or install software. There is fully access restriction to software and outside communications. A CIO explained this perspective very clearly: *"I prefer that my system is stopped than my system is insecure"*

4.2.2 Culture focused on individual contribution

In this culture, there are not any working constraints and individual initiatives are highly prioritized. In this case the users have the capacity and the responsibility of self-managing their security and they are allowed to access the information systems without

restrictions. This policy always creates users' discontent when implementing new security policies, since it supposes new restrictions.

4.3 Structure and involved people in security management

All the interviewed SMEs show a similar organizational information system security structure. None of the companies have an independent security department due to the company size. CIOs agree that it would be excessive to have a department dedicated to information system security.

Three different groups of people involved in these processes were identified:

- **System Administrators:** They lead the security management process and the company security depends on their awareness and knowledge.
- **Company executives:** The security is, generally, a priority for the company's executives who are aware of it and trust security managers but they usually lack of a deep knowledge about security. They are relevant because they usually decide the budget for the ISs department.
- **End users:** The end users think that security is an information system department responsibility and, as a result, they do not usually collaborate in the actions carried out to improve security in the company.

4.4 Most Common Security problems

- **Removable devices of high capacity:** USB ports and Pen drives allow the extraction of a large amount of information from the computers. Nowadays, USB keys have up to 1 GB capacity (or even more) and security managers struggle with data filtrations.
- **Information losses:** Backup systems facilitate data recovery. However, in order to carry out an efficient backup, the information should be on the right place in the computer network since backup copies are only carried out on some directories.
- **Passwords exchange:** All the interviewed managers admitted that although the users should not exchange passwords between them, many times they do.
- **Users' uncontrolled software installation:** Uncontrolled software downloads originate a decrease on the information systems' operability, new vulnerabilities and also legal conflicts due to unauthorized licenses.
- **Viruses:** They do not produce excessive losses of information because they are under control. Some SMEs have more than one antivirus and others have chosen alternative (and apparently more secure) operating systems such as Linux.
- **Spam:** Although in many SMEs it is not considered a security problem, spam is directly associated with e-mail. This problem affects all companies and it causes, mainly, time losses.
- **Phising:** website replacement, "fake Websites" is a way to obtain users' confidential data, harming users as well as e-businesses.
- **Law fulfillment:** Some SMEs, expressed the difficulty of meeting law fulfillment activities. They consider these activities, very complex, time consuming and difficult to get users involved.

- **Unauthorized backups:** SMEs' documents are printed and put on record in external and easily accessible places. These documents are not controlled and managers do not keep track of all copies.
- **Rudimentary backup copy mechanisms:** Some companies use rudimentary mechanisms to make backup copies such as Cds or other PCs. In those cases, no one takes any control on these storage devices, neither carry out periodic tests to ensure their functionality.

4.5 Case Study Best Practices

This 20 SME case study has allowed us to discover some security best practices that can be extended to other companies.

- **Allowing access to personal information through the Company Intranet**: Including confidential information in the intranet seems effective: *"Users do not share their passwords because they are worried about other workers accessing to their payrolls data"*.
- **Single sign-on**. Every worker has only one password to access to the system. "*Before this security mechanism, each user had several passwords (there are some users who have more than ten) and they usually had to write them down in order to remember"*.
- **Security committees**: These committees are formed by people from different areas. They have the responsibility of improving security aspects. These committees also allow spreading the security culture in the company.

5 Evolutionary phases

The current IS security management maturity differs from one firm to another, but its evolution has been analogous, although not all of them have reached the same maturity status. This evolution can be understood defining some phases: Growth, Integration, Formalization and Involvement.

Thus, the firms with the best security performance have passed through the previous, less mature stages. This process can also be seen as a learning process towards a more deep security comprehension.

These phases have not explicitly been mentioned by SME´s CIOs. They have been abstracted from the subsequent analysis of the interviews.

5.1 Growth phase

The business processes of the firms in this phase are not very dependent on their ISs. They could go on working several days even if the IS does not work properly. These firms have technical elements for security, as antivirus or firewalls. These elements work in an independent way without any formal management.

The ISs can be interconnected in many ways but there is not any well designed architecture. The security responsibilities are distributed, and each user has some responsibility securing the portion of the IS he/she uses.

The security controls are implemented when they are considered as something necessary. There are not planning activities and the control is almost inexistent. Firms in this stage do not see themselves as potential targets for attacks, neither external, nor internal.

Firms that are in this phase focus on a single aspect of security. This aspect can be confidentiality in some cases, recovery from information losses or law fulfilment in some others.

5.2 Integration phase

Businesses in this phase recognize the need for integrating their security elements in order to plan and control them. They realize that trying to secure a mess makes no sense. Security reasons are not the only ones that drive firms towards a more coherent IS architecture. The specific goal is to accurately design the system's architecture that will be secured.

During this phase, firms gain a broader perspective over security and recognize the different elements that are included in. They also get a deeper understanding about each element and its interrelations with others.

Firms in this phase usually concentrate their information in servers. This makes its protection far easier. Nevertheless, since all the information has been concentrated in the same place, any attack against this info-centre would be critical for the organization. As a result, even though the probability of an incident has been reduced, the severity of the consequences has increased. This risk increase increments the commitment to security. Another example of this phase could be the single sign-on mechanism, which has been explained in the Best Practices section (4.5).

5.3 Formalization phase

Once the system to be secured has been accurately designed and implemented, the effectiveness of security depends mainly on its management. Firms already possess the required technical media to guarantee their security, now they have to use them correctly. They develop some procedures and assign responsibilities to achieve this goal.

Some of the interviewed companies do not use reference models and their security actions are based on common sense or on CIO's individual knowledge. In a few cases companies attend courses and consult specialized books with the purpose of delving deeper into security. Software and hardware suppliers also help companies to develop their security management model.

Some other SMEs decide to outsource their entire IS management. As a consequence, there will be a dependency on the outsourced firm and the security model will be designed to the liking of the outsourced firm. This partnership is not always the same. Some companies audit the outsourced firms and others hardly carry out monitoring actions. Some SMEs decide not to outsource the IS management but they base their security improvement actions on external audits.

Without a doubt, the companies that use a reference model have achieved better results on security management of information systems. The adopted model can be based on the ISO 17799, Spanish data protection law (LOPD) or on the SOA (Sarbanes-Oxley Act) law. In all these cases, companies have adopted a reduced version of these reference models. Although the certification achievement is not a high priority, companies usually keep in mind the ISO recommendations when they are developing their models.

5.4 Involvement phase

Users can behave against security mechanisms if they see them as an obstacle for their daily work. Even if the firm uses a proper security system, people can always be the weakest link. Communication and education are necessary to build up a security culture, where it is considered a beneficial value for the firm.

In this phase, security is integrated in people's routines. It is taken into account when decisions are made. People understand the relevance of security and also why they have to accomplish the established controls. They realize that security controls are there to avoid problems in the next future.

There are some tools that can be considered as successful mechanisms for the firm in this phase. The creation of multidisciplinary committees to design security, including people from IS department but also project managers and base users. Another good practice consists of including security aspects on the welcome activities of the first working day.

Firms finally recognize that growthl, integration, formal and involvement efforts are necessary to deploy an efficient security. The absence of any of these efforts could cause breaches.

6 Explaining security management evolution through mental models

The four phases mentioned in the previous section can be more deeply understood analysing the mental models of CIO's. This analysis has been developed through causal loop diagrams and behaviour over time graphs, with the intention of capturing both structure and behaviour. This work can also be seen as an example of measuring learning through the mental model analysis (Schafernitch, 2004).

The mental model concept has a long tradition on System Dynamics literature (Doyle et al., 1998). System Dynamics practitioners know that the human minds are one of the richest sources of knowledge for modelling. Making CIOs' mental models explicit could be a good alternative to gain a better understanding about SMEs' security management and its evolution.

6.1 Stage 1: Growth phase mental model

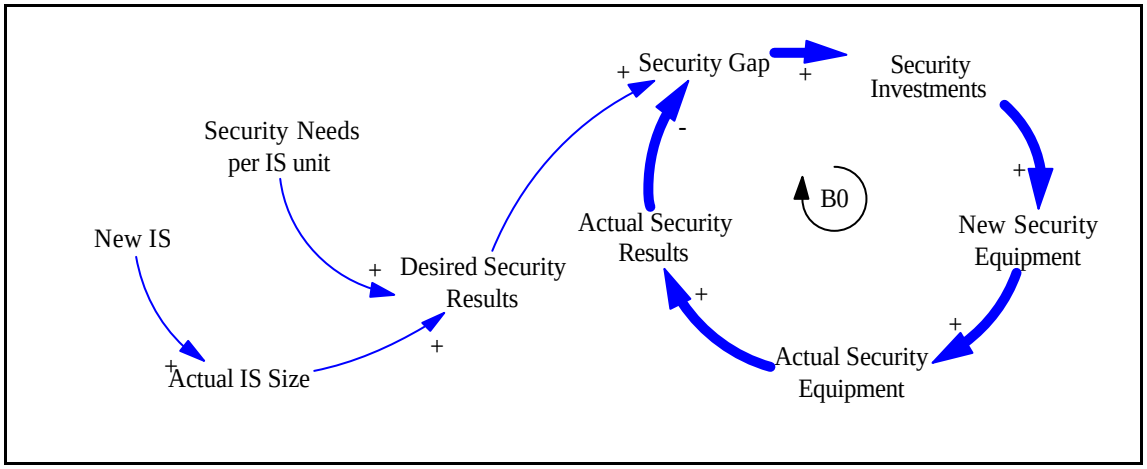

Figure 1: Phase 1, solution loop

CIOs recognize the security needs and begin to acquire and implement the first pieces of security equipment, such as antivirus software or firewalls. The associated mental model is quite simple: every time there is a new security need, the problem is solved through a single balancing loop (see loop B0 in Figure 1). Thus, the security needs are analysed independently.

There is a pure technical conception about security. This mental model responds to this simple reasoning, *"More security controls I have, more secure I am"*. The security controls are implemented in an urgent way, with no planning.

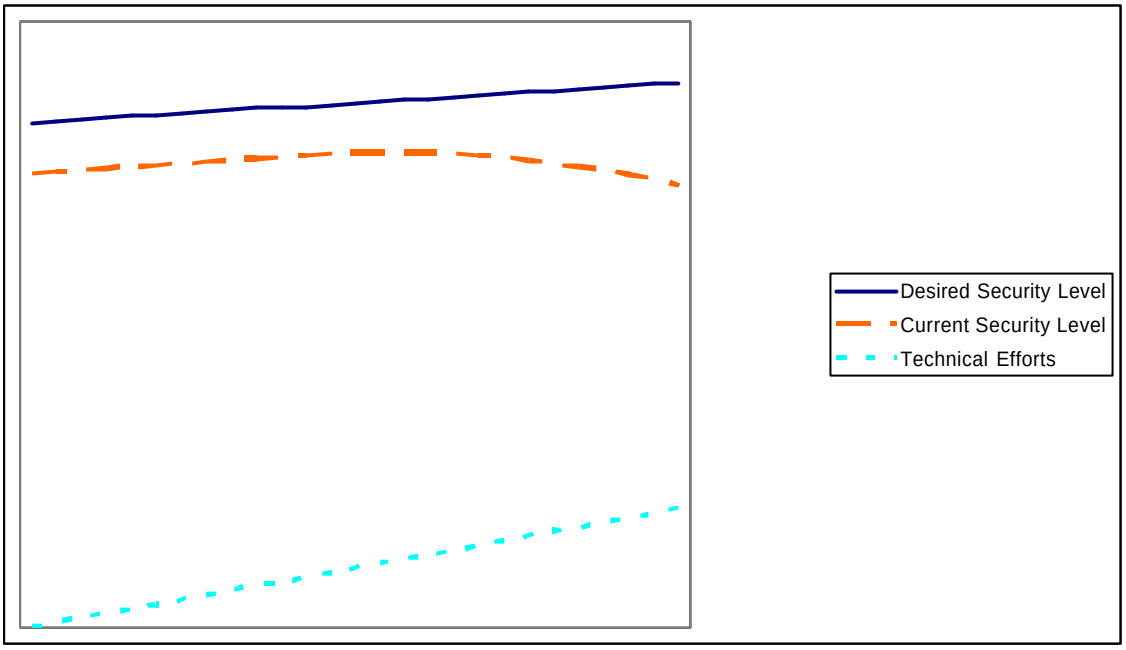

Figure 2: Behaviour of the phase 1

This security strategy is valid for a while, but the obtained security results decrease (Figure 2). The implementation of independent technical controls is not longer enough to achieve the desired security level.

6.2 Stage 2: Integration phase mental model

The problem of being absolutely reactive is understood. Acquiring new security equipment is not enough, because when the size of the installed base increases, integration problems appear (see loop R1 in figure 3). Having all these security tools creates inefficiencies due to lack of integration that prevent their efficient use. The problem is not the absence of security equipment, but its incorrect deployment. The key aspect of this second stage is integrating the already implemented and the future security equipment.

The solution to the previous situation is the focus on integration. The effort to secure every isolated IS is huge. The ISs and the securing mechanisms should be correctly integrated in order to get satisfactory results. This is explained by the loop B1in figure 4.

These efforts can be triggered by the firm's ISs upgrades. Some firms were updating or installing a new ERP when they realize the relevance of security, typically influenced by their ERP providers. Thus, implementing new ISs boosts security.

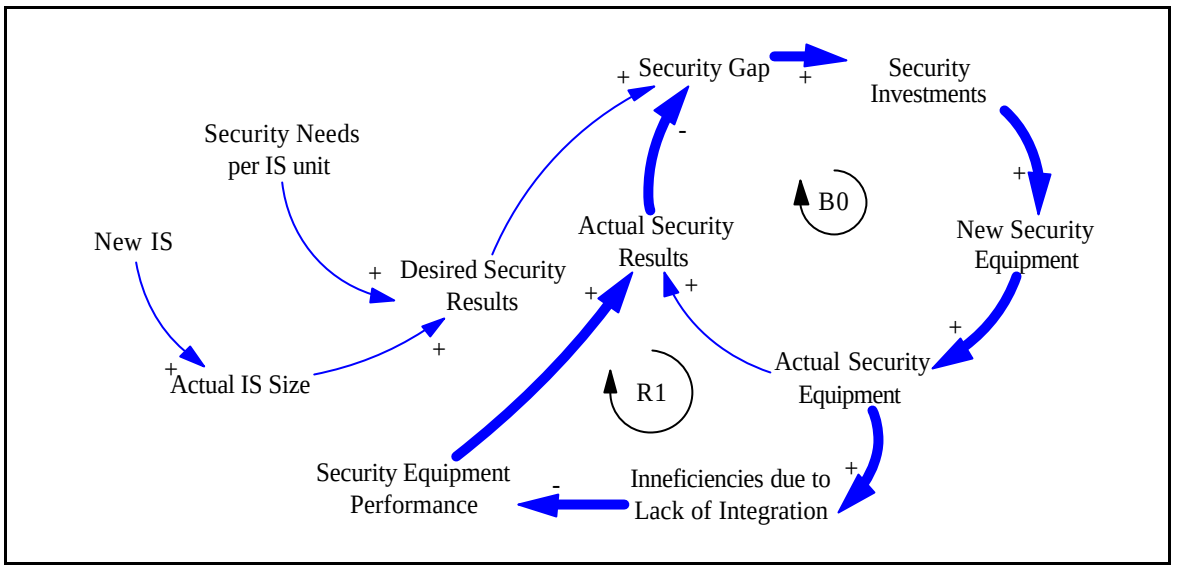

Figure 3: Phase 2, problem loop

The influence of ISs' providers also implies a broader perspective about security. Every security element is observed as a mechanism conforming the firm's security structure. The "Defences in depth" concept is understood (Reason, 1997). This implies that successive layers of protection are implemented co-ordinately, one behind the other, each guarding against the possible breakdown of the one in front. Some firms were already using several antiviruses.

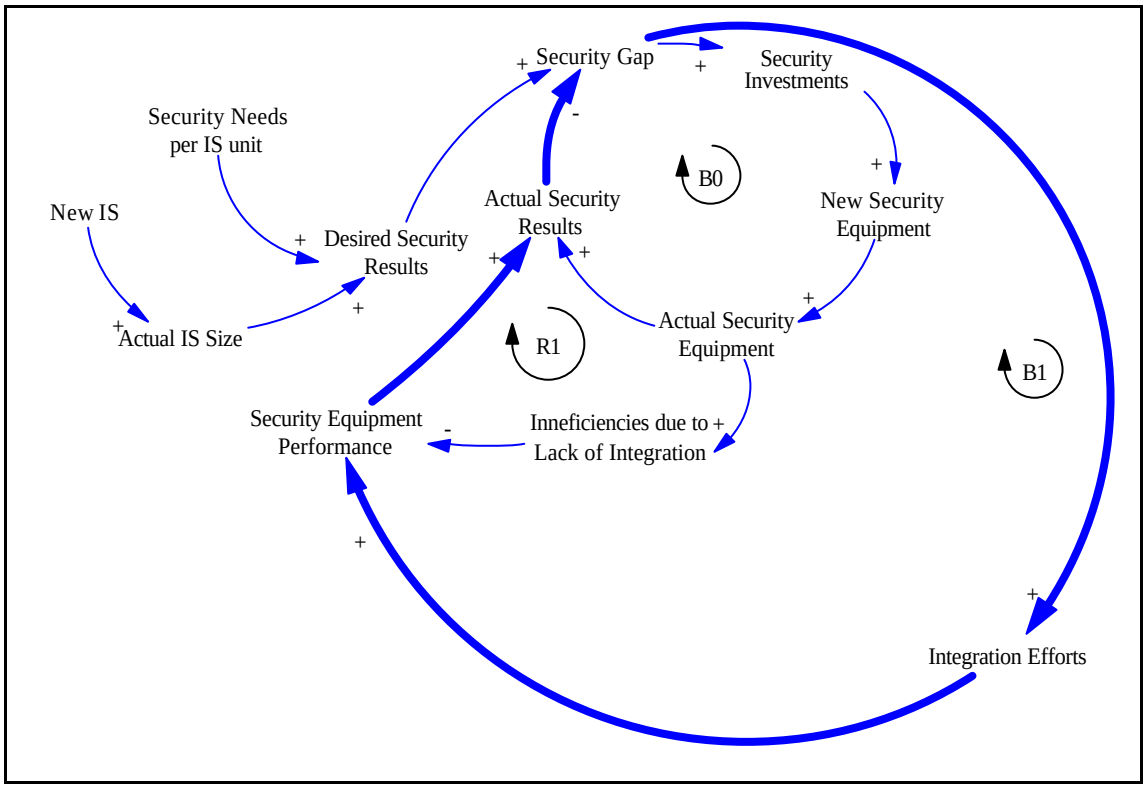

Figure 4: Phase 2, solution loop

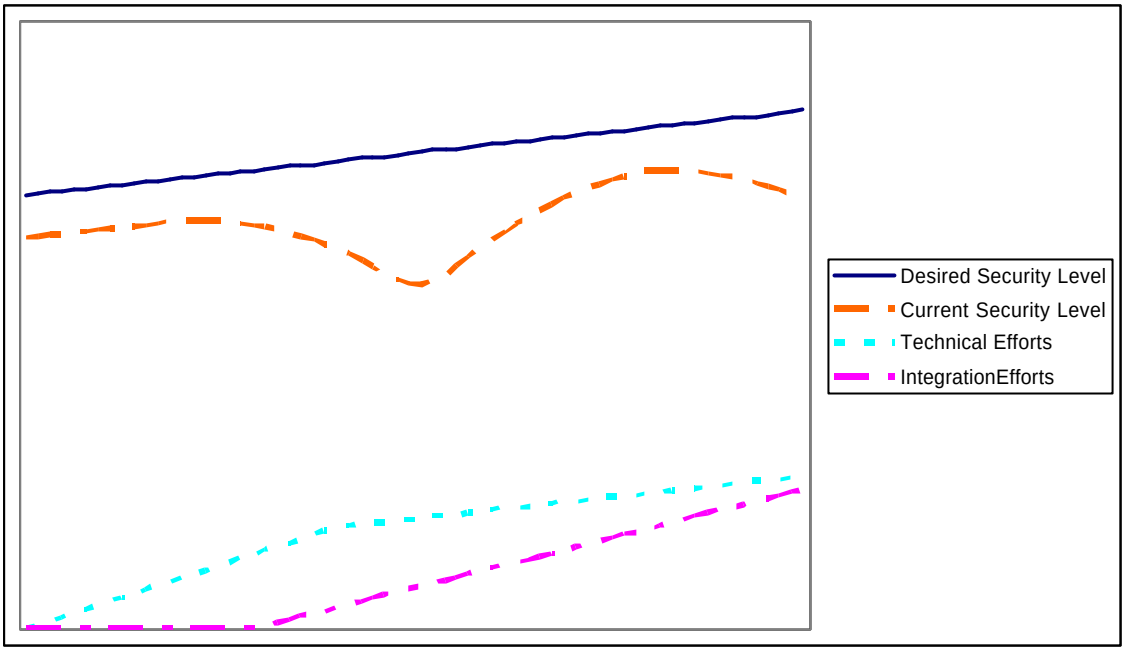

Figure 5: Behaviour of the phase 2

The security improves with the integration efforts, but this tendency changes again (see figure 5). The IS department collapses due to personnel scarcity. A CIO claimed: *"We've got a firewall, a log recorder, some antiviruses, and an intrusion detection system. All of them provide very interesting information...but I've no time to analyse it!"*

6.3 Stage 3: Formalization phase mental model

Once the IS and the securing mechanisms have been integrated, the security of the firm improves. But there is a new constraint for this system. Security mechanisms need to be managed in order to work efficiently. The tools are present, but there are not enough resources to plan their activities and to analyse the results they offer.

Security does not reach the desired level because of this lack of formalization (See loop R2 in Figure 6). As the security architecture growths, it becomes more unmanageable.

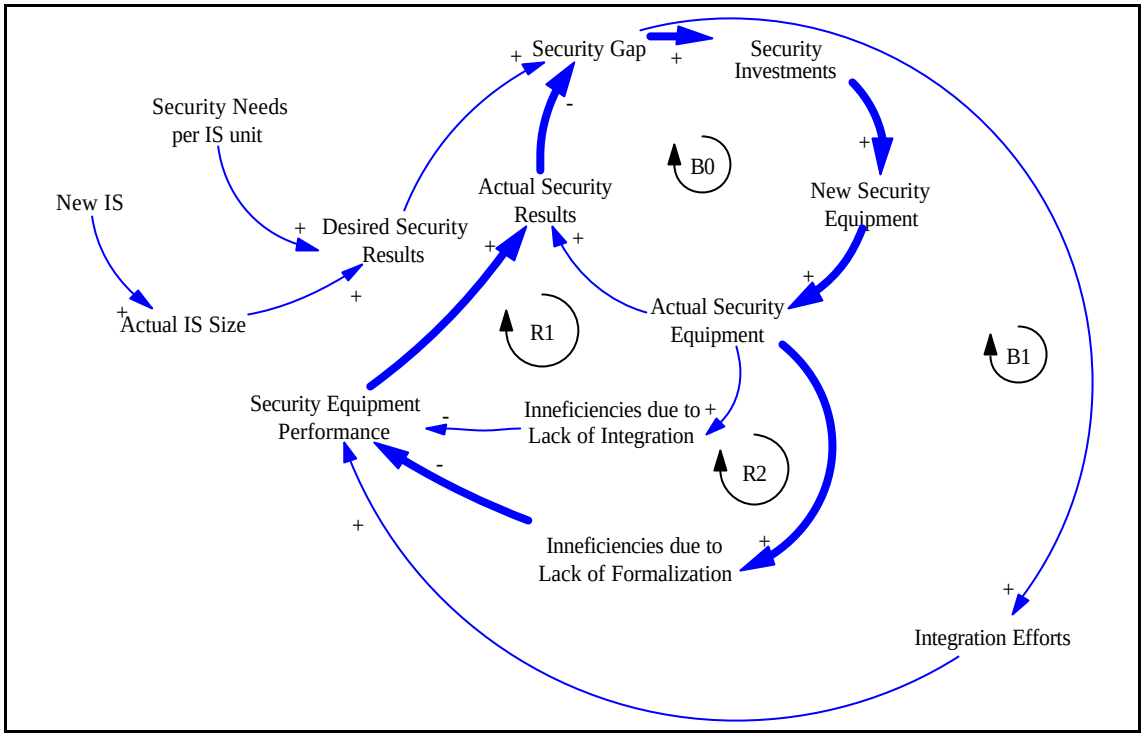

Figure 6: Phase 3, problem loop

The formalization efforts of the firm guarantee that the required resources will be ready when they are needed. Some procedures are developed; planning and monitoring mechanisms are designed and implemented. The size of the IS department can increase a bit to afford the new responsibilities. Some activities can be outsourced, such as auditing processes.

In this phase, formal management efforts are developed (see B2 in figure 7), such as more structured methodologies for risk analysis, indicators for security control, cross-supervision responsibilities, back up protocols and contingency plans.

The CIO´s work moves from a purely technical one to a more managerial one. This step is not easy for SME´s CIOs. They usually present a technical profile and have not developed managerial skills. They see themselves as technicians, not as managers.

This evolution has also happened to analogous professions. It is not until recently that analytical, technical, managerial and interpersonal skills were required for succeeding as an IS analyst (Hoffer et al., 2002).

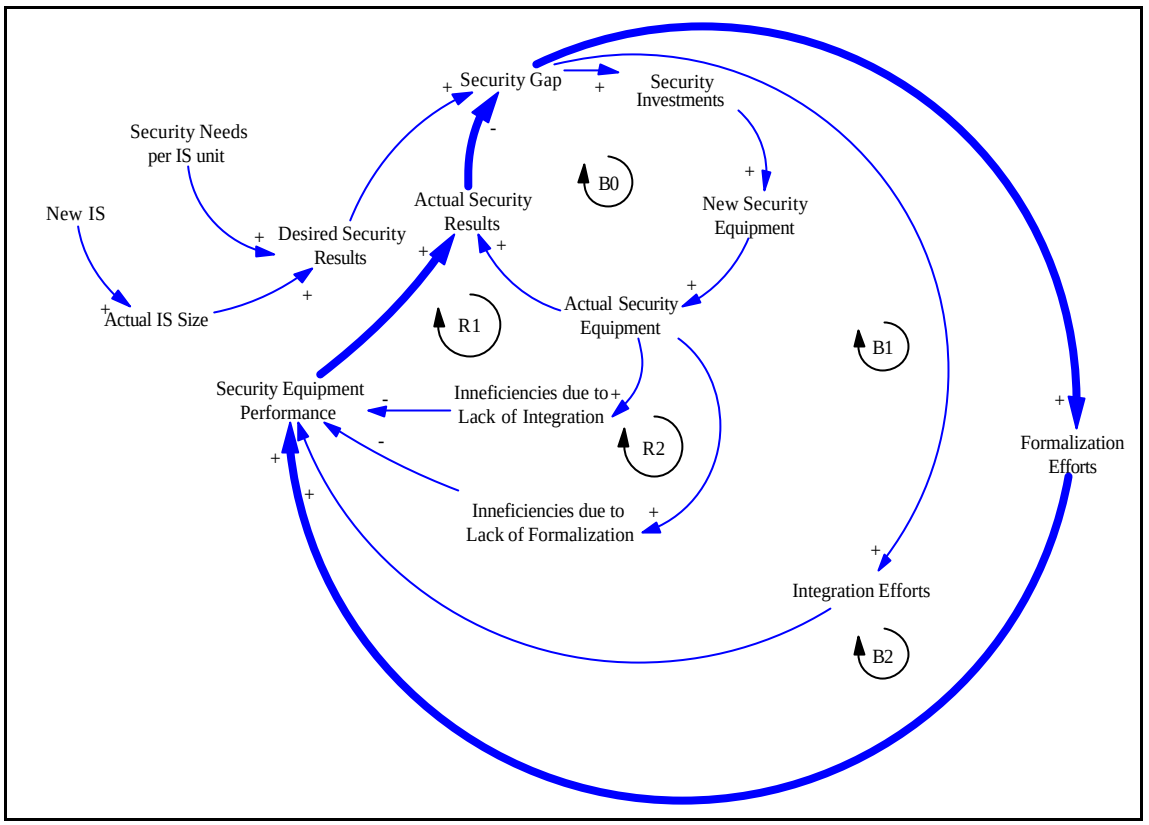

Figure 7: Phase 3, solution loop

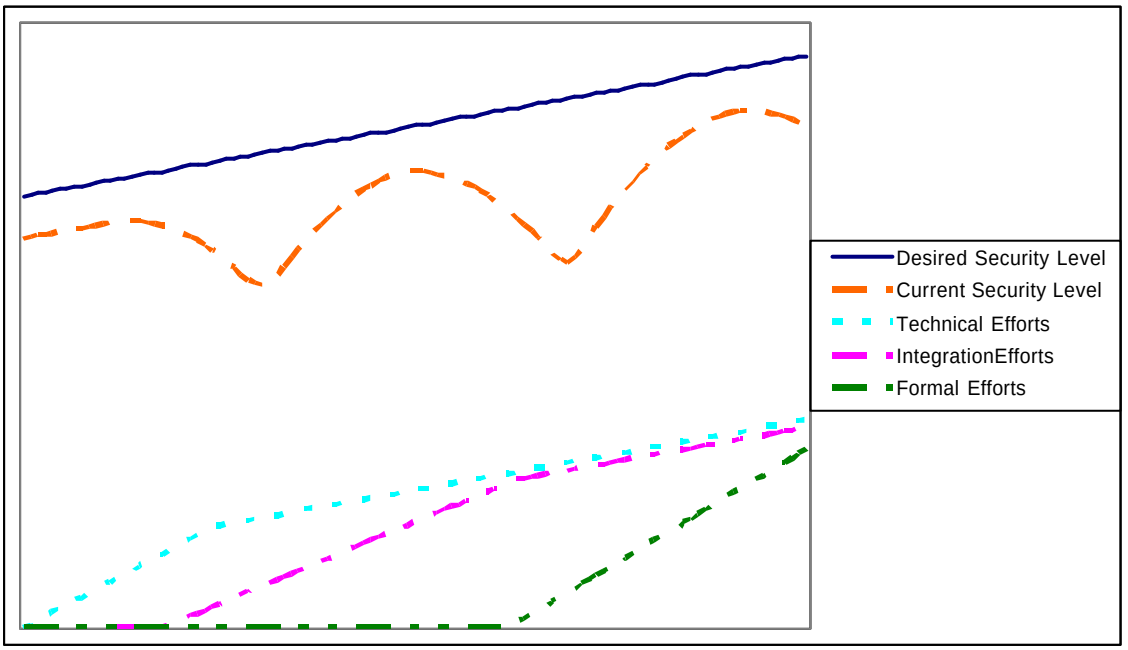

Figure 8: Behaviour of the phase 3

Once the procedures have been defined and some planning about resources and control mechanisms exist the behaviour improves. The efforts are directed towards efficient actions and wastes are diminished.

The behaviour improves but it falls again when the formalization efforts are not enough to reach the desired security level (see figure 8)

6.4 Stage 4: Involvement phase mental model

The next problem is related to people. Workers can observe security mechanisms as constraints to their work. Perhaps, they do not understand the root reasons of these controls. They also could superstitiously learn that the security controls are excessive. These behaviours can generate dangerous breaches in security. This is represented through loop R3 in figure 9.

The already designed formal controls can be weakened because of the lack of acceptance. Some of the CIOs have spoken about the users as "*the enemy*". People can make any security measure ineffective. Some security culture is essential. If security measures are perceived as obstacles they can not be maintained over time. The already designed formal controls can be weakened because of the lack of involvement.

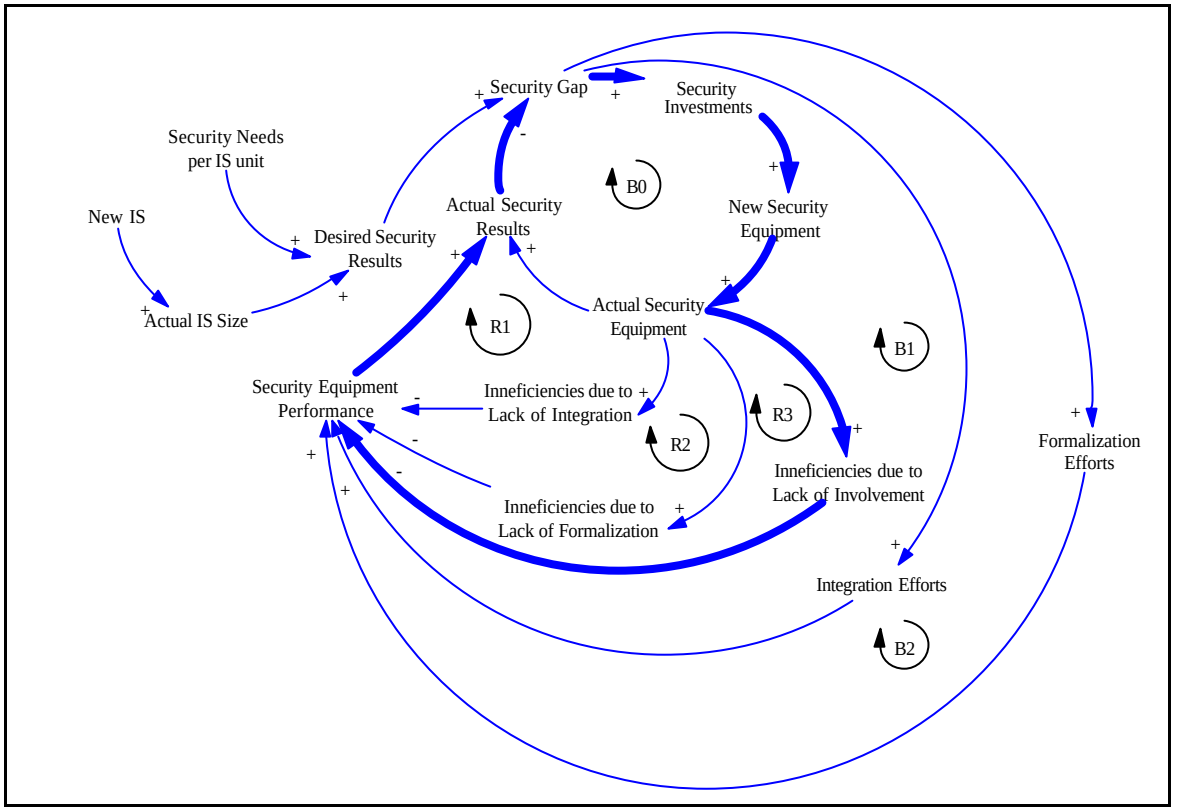

Figure 9: Phase 4, problem loop

Involvement efforts are developed to go beyond theses difficulties (See loop B3 in figure 10). The reasons for implementing security controls are explained to workers.

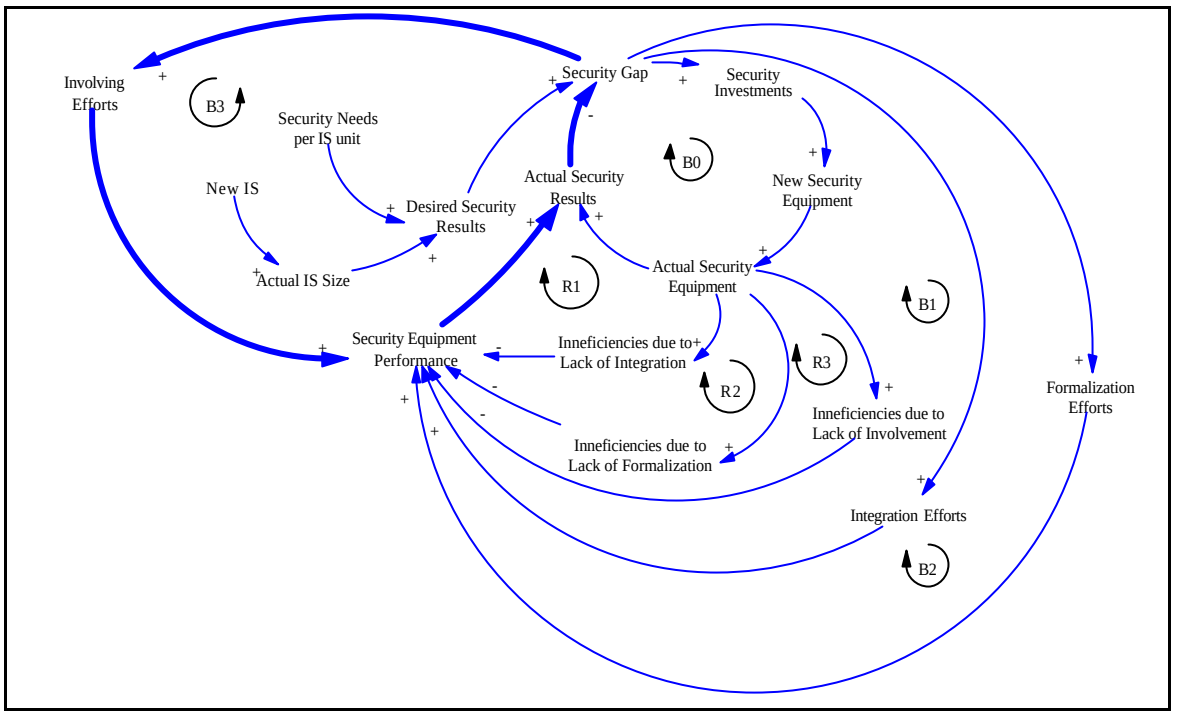

Figure 10: Phase 4, solution loop

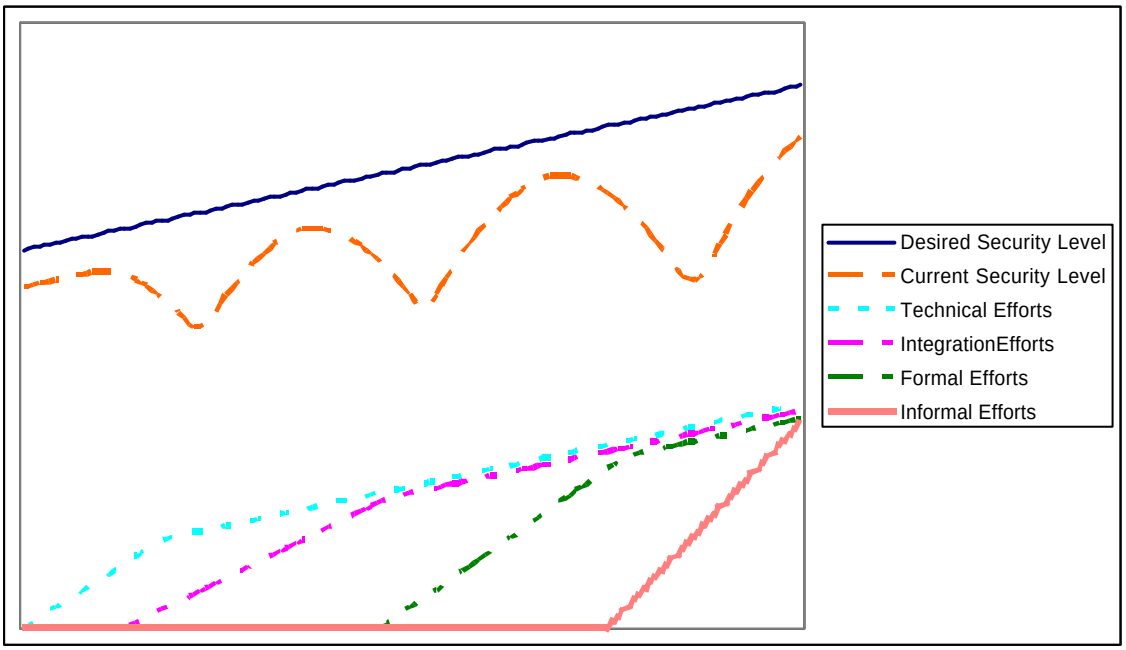

Figure 11: Behaviour of the phase 4

The recognition of the relevance of all the efforts, technical, integration, formal and involving leads the firm towards the desired security level. Or, like a CIO explained "*towards the minimal insecurity level*".

All the CIOs recognize that total security is not possible. One of them said that "*Total security would have infinite costs*". But, if technical, integration, formal and informal efforts are in equilibrium there is a chance for security.

7 Conclusions

The evolution of the information systems management onto 20 Basque SMEs has been analysed. There have been identified four phases in this evolution and the characteristics of each phase have been presented. All this has been explained making explicit the manager's mental models associated to each phase using causal loop diagrams and behaviour over time graphs

The majority of the analysed firms could be placed around the second phase. They are still integrating their ISs and the recognition of the need for strong formalization efforts is only in CIO's minds.

Archetypes can also be useful to understand these behaviours. (Wolstenholme, 2004). The presented evolutionary stages can be considered as different instances of the same "out of control" archetype.

Security needs to be integrated within other IS requirements. There is no possibility of creating a security department onto SMEs in the short term. The security responsibility should be shared with other into the ISs department.

More quantitative approaches would be very positive, but there is very few data. There are several reasons for this data scarcity: on one hand, it is difficult to measure some of the main variables of the system. On the other hand, there are confidentiality reasons that avoid the public disposal of data. Anyway, security management is already a main concern for firms, and it will increase in the very close future.

8 References

Anderson, R. (2001). Security Engineering, New York, NY: John Wiley& Sons, Inc

Brancheau, J.C., Janz, B.D., Wetherbe, J.C., (1996), Key issues in information systems management: 1994-95 SIM Delphi, MIS QUARTERLY 20 (2): 225-242

Certification Europe, (2004), http://certificationeurope.com/services/downloads.asp

Corporate Information Security Working Group, Information Security Management References, Adam H. Putnam, Chairman; Subcommittee, U.S. House of Representatives, March 18, 2004.(available from http://reform.house.gov/UploadedFiles/Best%20Practices%20Bibliography.pdf)

COBIT Online, www.isaca.org/cobitonline

Dhillon G., J. Backhouse (2001): Current directions in IS security research: towards partner-organizational perspectives. Info Systems Journal (11) pp 127-153

Doyle, J. K., Ford, D. N., (1998), Mental models concepts for system dynamics research, System Dynamics Review 14, 1, 3-29

Ford, D. N., Sterman, J. D., (1998), Expert Knowledge elicitation to improve formal and mental models, System Dynamics Review 14, 1, 309-340

Gonzalez, J. J., Sawicka, A., (2003), The Role of Learning and Risk Perception in Compliance, Proceeding of the 21st International Conference of the System Dynamics Society, New York (USA)

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., 2004 CSI /FBI Computer Crime and Security Survey, Computer Security Institute Publications

Hoffer, J. A., George, J. F., Valacich, J. S., (2002), Modern System Analysis & Design, Prentice Hall, New Jersey

Kumar, V., Maheshwari, B., Kumar, U., (2003), An investigation of critical management issues In ERP implementation: an empirical evidence from Canadian organizations, Technovation 23, 793-807

LOPD, Ley Orgánica de Protección de Datos de caracter personal, (1999), (available from http://www.belt.es/legislacion/vigente/sp_pcivil/spublica/videovigilancia/pdf/lo_15_lopd.pdf)

Mylopoulos, J., Chung, L., Nixon, B., (1992), Representing and Using Nonfunctional Requirements: A Process-Oriented Approach, IEEE Transactions on Software Engineering, 18, 483-497

Price Waterhouse Coopers, Information Security Breaches Survey 2004, available from http://www.pwc.com/images/gx/eng/about/svcs/grms/dti_databackups_final.pdf

Ranganathan, C., Kannabiran, G., (2004), Effective Management of information system function: an exploratory study of Indian organizations, International Journal of Information Management 24, 247-266,.

Reason, J., (1997), Managing the Risks of Organizational Accidents, Ashgate, Hants (England)

Remenyi, D., White, T., Sherwood-Smith, M., (1999), Language and a post-modern management approach to information systems, International Journal of Information Management 19, 17-32

Rudolph, K., Warshawski, G., Numkin, L., (2002), Security awareness, in Computer Security Handbook, ed. by Bosworth, S. and Kabay, M. E, John Wiley and Sons Inc., Fourth edition, New York (USA)

Sarbanes-Oaxley Act of 2002 (Available from http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf)

Schaffernicht, M, (2004), Do models evolve?, Proceeding of the 22nd International Conference of the System Dynamics Society, Oxford (UK)

Schneier, B. (2003). Beyond Fear 1 ed. New York, NY: Copernicus Books

The ISO 17799 Service & Software Directory, www.iso17799software.com

Torres, J. M., Sarriegi, J. M., (2004), Dynamic Aspects of Security Management of Information Systems, Proceeding of the 22nd International Conference of the System Dynamics Society, Oxford (UK)

Wolstenholme, E., (2004), Using generic archetypes to support thinking and modelling, System Dynamics Review 20, 4, 341-356