CORE
Metadata, citation and similar papers at core.ac.uk
Provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings | Proceedings

An Analysis of and Perspective on the Information Security Maturity Model: a case study of a Public and a Private Sector Company

Lucio Silva
Federal University of Pernambuco, Recife, Brazil., lucio_camara@hotmail.com

Thiago Poleto
Federal University of Pernambuco, Recife, Brazil., thiagopoleto@hotmail.com

Jadielson Moura
Federal University of Pernambuco, Recife, Brazil., dielson10@hotmail.com

Ana Paula Costa
Federal University of Pernambuco, Recife, Brazil., apcabral@hotmail.com

Follow this and additional works at: http://aisel.aisnet.org/amcis2012

Recommended Citation
Silva, Lucio; Poleto, Thiago; Moura, Jadielson; and Paula Costa, Ana, "An Analysis of and Perspective on the Information Security Maturity Model: a case study of a Public and a Private Sector Company" (2012). *AMCIS 2012 Proceedings*. 11.
http://aisel.aisnet.org/amcis2012/proceedings/PerspectivesIS/11

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

An Analysis of and Perspective on the Information Security Maturity Model: a case study of a Public and a Private Sector Company

Lúcio Silva
Federal University of Pernambuco
lucio_camara@hotmail.com
Thiago Poleto
Federal University of Pernambuco
thiagopoleto@hotmail.com
Ana Paula Costa
Federal University of Pernambuco
apcabral@hotmail.com
Jadielson Moura
Federal University of Pernambuco
dielson10@hotmail.com

ABSTRACT

Information Security (IS) is a concept that is related to protecting a set of data in order to preserve the value it has for an individual or an organization. A review of the literature shows there are four main aspects related to IS: confidentiality, integrity, availability and non-repudiation. Based on these four aspects, a new framework is put forward for analyzing the information security maturity model (ISMM) in an organization, assuming that each organization has a minimum level of information security policies in each aspect, taking into consideration the percentage of policies that this organization has from all those cited in our model. At the end, a case study was conducted in order to analyze the ISMM of a public and private sector company.

Keywords

Information security, information security policies, maturity model.

INTRODUCTION

As a result of globalization and new forms of fierce competition this has generated, information has come to be regarded as a capital value, which makes it a key resource in competitiveness, profitability, and essential for revealing gaps in the market.

Therefore, companies have seen the information as an asset that can lead to outstanding success (Straub, 1990; McFadzean, Ezingeard and Birchall, 2007).

However, given the growth in data in business environments in recent years, organizations depend largely on computer-based Information Systems (IS) for vital parts of their operations. Yet institutions worldwide face increasing security threats that can undermine the operation of these systems. Therefore, organizations need security controls to protect the information they value most.

Organizations need to minimize the vulnerability of such information to being improperly accessed or used, leaked, stolen, copied, lost, corrupted or repudiated by adopting information security policies. According to Shirtz and Elovici (2010), information security is related to four aspects: confidentiality, integrity, availability and non-repudiation. Confidentiality means that all information should be protected in accordance with the degree of confidentiality of its content, and that the way in which its contents are displayed should be limited. Integrity is associated with the state of information at the time it is generated and when retrieved. It will be a complete retrieval if the information is faithful to its original state. Availability ensures that only authorized users have access to information and the corresponding systems when they need them. Non-repudiation is the assurance that someone cannot deny something and refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of his/ her signature on a document or the sending of a print message that he/ she originated.

Based on these four aspects, a new framework is put forward for analyzing an information security maturity model (ISMM) in an organization, assuming that each organization has a minimum level of information security policies in each aspect, taking into consideration the percentage of policies that this organization has from all those cited in our model.

The rest of the paper is organized as follows: Section 2 is dedicated to a review of the literature on information security policies; Section 3 presents the building blocks of our methodology. This begins with a short discussion on how the information security policies that have been proposed for our particular evaluation task were chosen; Section 3.1 reminds the reader of the terminology of SODA; Section 3.2 describes the structure of the model; Section 3.3 describes the methodology proposed to analyze the ISMM based on an additive model and details all aspects considered; Section 4 provides a case study of the proposed methodology and discusses the results. Finally, the conclusions of this work are presented in Section 5 which also makes recommendations for further research studies on this topic.

A BRIEF REVIEW OF THE LITERATURE

Several models and frameworks have been suggested for the process for taking remedial action when information security events occur.

Veiga and Eloff (2010) propose a framework used for assessing the information security culture in an organization, by taking account of the technical, procedural and human behavioral components. It also provides an all-encompassing and single point of reference for cultivating a culture in an organization that minimizes the risks posed by employees' behavior.

Shirtz and Elovici (2010) propose a new framework for optimizing investment decisions when taking decisions on information security remedial actions. Their framework assumes that the organization is aware of a set of remedial actions that can be used to address end-effects that have been identified and the framework is used to identify the optimal set of such actions for a given budget that complies with the organization's information security policy.

In another study, Marciano and Marques (2006) take a social approach to information security, pointing to alternative strategies for drawing up security policies. Initially interviews were conducted with users and managers of information systems in order to assess their perception of information security. However, the responses were speculative in the sense that the subject had not been previously discussed within the organization. Subsequently, proposals were made to formalize information security policies through mechanisms of logic, with a view to eliminating ambiguities regarding the computational handling of these policies in organizational environments.

The study by Moreira, Martimiano, Brandão and Bernardes (2008) focuses on the technological aspects of security, and presents an overview of the impacts and ways to address security within an organization, and stresses that this task is complex. Matushima, Venturini, Sakuragui, Carvalho, Ruggiero, Naslud and Pourzandi (2006) specifically discuss issues related to access control, which led them to drawing up a framework that addresses issues of authentication, security and privacy of communication and enforcing access control in a transparent manner.

Yayla (2011) creates a framework to reduce intentional and unintentional insider threats by investigating the underlying causes of these threats, and emphasizes the reinforcing and integrative roles that information security policies play in achieving effective control in organizations.

Knapp, Morris, Marshall, and Byrd (2009) proposed a model that reflects an information security policy process in modern organizations based on recommended practices from a sample of certified information security professionals. The model evolved from the data and used qualitative techniques to identify the primary policy processes, the key environmental and organizational influences, and the underlying linkages among them. It also holds out the promise of providing relevant guidance for practice and theoretical insight for research.

In order to describe the four aspects (Shirtz and Elovici, 2010), the following table summarizes information security policies (ISP), extracted after an extensive review of the literature, in accordance with each aspect.

Drawing on the literature, Table 1 presents a summary of different authors' views on information security policies. The list of authors is not exhaustive but it does give a glimpse into the diverse literature on information security. Some of these authors base their views on empirical research and others base their views on experience and theory only. In order to facilitate the application of the model throughout this paper, next to each policy in Table 1, there is an acronym for each information security policy inside each aspect. For example,"Encrypton of data at rest" is the first policy of confidentiality (PC_1). Following this reasoning, PI, PA and PN represent, respectively, policies of integrity, availability and non-repudiation.

Confidentiality		**Integrity**	
ISP	References	ISP	References
Encryption of data at rest (PC_1)	Askarov and Sabelfeld (2007); Bacik (2008); Byun and Lee (2011); Shirtz and Elovici, (2010)	Monitoring System (PI_1)	Bacik (2008); Daniela (2011)
Authentication of User ID for digital signature, and Lock account (PC_2)	Bacik (2008); Harn and Ren (2011); Zhang, Li and Song (2011)	Backup (PI_2)	Jayadevappa and Soh (2009); Tomono, Inutake, Uehara, Shimada, and Yamagiwa (2010); Yang , Shieh and Leu (2009); Zhongmeng and Hangtian (2010);
When surfing the Web, does not allow browsers to accept cookies from Web sites / Session Management (PC_3)	Ayadi, Serhrouchni, Pujolle and Simoni (2011); Bacik (2008); Guzman, Galvez, Santon and Stam (2010)	Server and WS antivirus (PI_3)	Shirtz and Elovici, 2010; Vasilyevna, Yeo, Cho and Kim (2008); Zhang and Shuai (2009); Wei, Hwang and Chin (2011);
Authentication Protocol for RFID System (PC_4)	Wei et al. (2011)	Mail antivirus (PI_4)	Shirtz and Elovici, (2010)
Scan attacks (PC_5)	DaRolt, Di Natale, Flottes and Rouzeyre. (2011)	Physical security of the environment (PI_5)	Yang et al. (2009);
Develop what-if scenarios on information security and risk, leverage the knowledge of specialists (PC_6)	Williams (2001)	Applications and candidate detectors (PI_6)	Kayacık, Zincir-Heywood and Heywood (2011)
Create an audit committee that clearly understands its role in information security and how it will work with management and auditors (PC_7)	Williams (2001)	Defense strategy wireless networks (PI_7)	Chen and Leneutre (2011)
		Application firewall (PI_8)	Chiong and Dhakal, (2008); Yang et al. (2009)

		Strengthen all security and critical server and communications platforms (PI_9)	Williams (2001)
Availability		**Non-Repudiation**	
ISP	References	ISP	References
Identification of user accounts (PA_1)	Bacik (2008)	Communications and operations management (PN_1)	Yang et al. (2009)
Access and control - Restriction on user accounts (PA_2)	Bacik (2008); Faravelon, Verdier and Front (2011)	Classification of Information on the value for the organization (PN_2)	Yang et al. (2009)
Limitations on access and monitoring external IDs and IP (PA_3)	Bacik (2008)	Traffic Analysis (PN_3)	Chaum (1981)
All of my computer sessions require a unique user-id and password (PA_4)	Guzman et al. (2010)	Security Policy Role and responsibilities for information security (IS) (PN_4)	Yildirim, Akalp, Aytac and Bayram. (2011)
Radio Frequency Identification (RFID) (PA_5)	Pietro and Molva (2011)	Staff have been trained to secure their computers at all times (PN_5)	Yildirim et al. (2011)
Evaluates the effects of an information security awareness programme (PA_6)	Albrechtsen and Hovden (2010)	Run security responsiveness programmes, establish security baselines and rigorously check compliance (PN_6)	Williams (2001)
		Risk Assessment (PN_7)	Burke (2009)

Table 1. Summary of Information Security Policies (ISPs)

THE PROPOSED MODEL

One of the main objectives of information security policies is to provide an organization with guidelines and set of rules to prevent security breaches. To draw up the model, the steps shown in Figure 1 were followed.

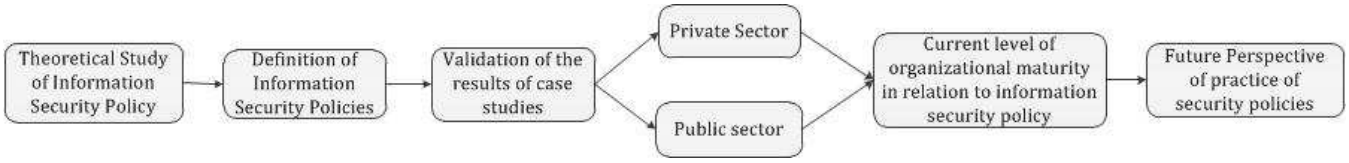

Figure 1. Steps followed when drawing up the model

As a first step, a theoretical basis for information security policies was generated by conducting a survey of the literature on this topic. In particular, this review enabled a wide range of policies to be defined that can be adopted in companies. A meeting was held with specialists from two different companies, one from each of the public and private sectors, to validate these policies. Then, the maturity level of each of the companies was determined. Based on this level of maturity, the likelihood of the company adopting new policies in future can be calculated with a view to ensuring that the company is up to date on information security matters.

Context of the Problem

Information security governance has become a very focused activity. According to Williams (2001), information systems can generate many direct and indirect benefits, and as many direct and indirect risks. In order to mitigate these risks, there are several policies and plans for IT security that companies can adopt, as can be seen in Table 1. The more of these an organization adopts, the less vulnerable to loss of information it becomes.

However, an organization needs to reach a better understanding of the importance of using information security policies, the threats that they are vulnerable to, and so on. Besides, it is very difficult for only one decision-maker to consider all the important aspects of a problem since the complexity of socioeconomic environments has greatly increased (Kim and Ahn, 1999).

Strategic Options Development and Analysis – SODA - aims to provide decision makers with a better understanding of the problem, which is made possible because there is greater interactivity. The methodology is based on constructing cognitive maps of the actors involved in decision making.

According to Eden and Ackermann (1998), the process can be developed in a few steps: the facilitator defines the problem; from this definition the actors identify an alternative that is its opposite so the facilitator will build a map of each actor later. In this step the workshop phase takes place during which new concepts can be removed or added.

Structure of the Model for Information Security Policies

The model used was based on the methodology of Strategic Options Development and Analysis (SODA), using cognitive maps (Ackermann, Eden and Cropper, 1995). Adopting this methodology will give members a greater understanding of the problem.

However, the process of constructing the maps will not be discussed in this paper. The cognitive map is a way of trying to grasp different ways of thinking and to involve all partners to redefine the problem perceptions and form grounds for commitment and consensus decisions. Therefore, in this case, the problem is to maximize the use of information security policies.

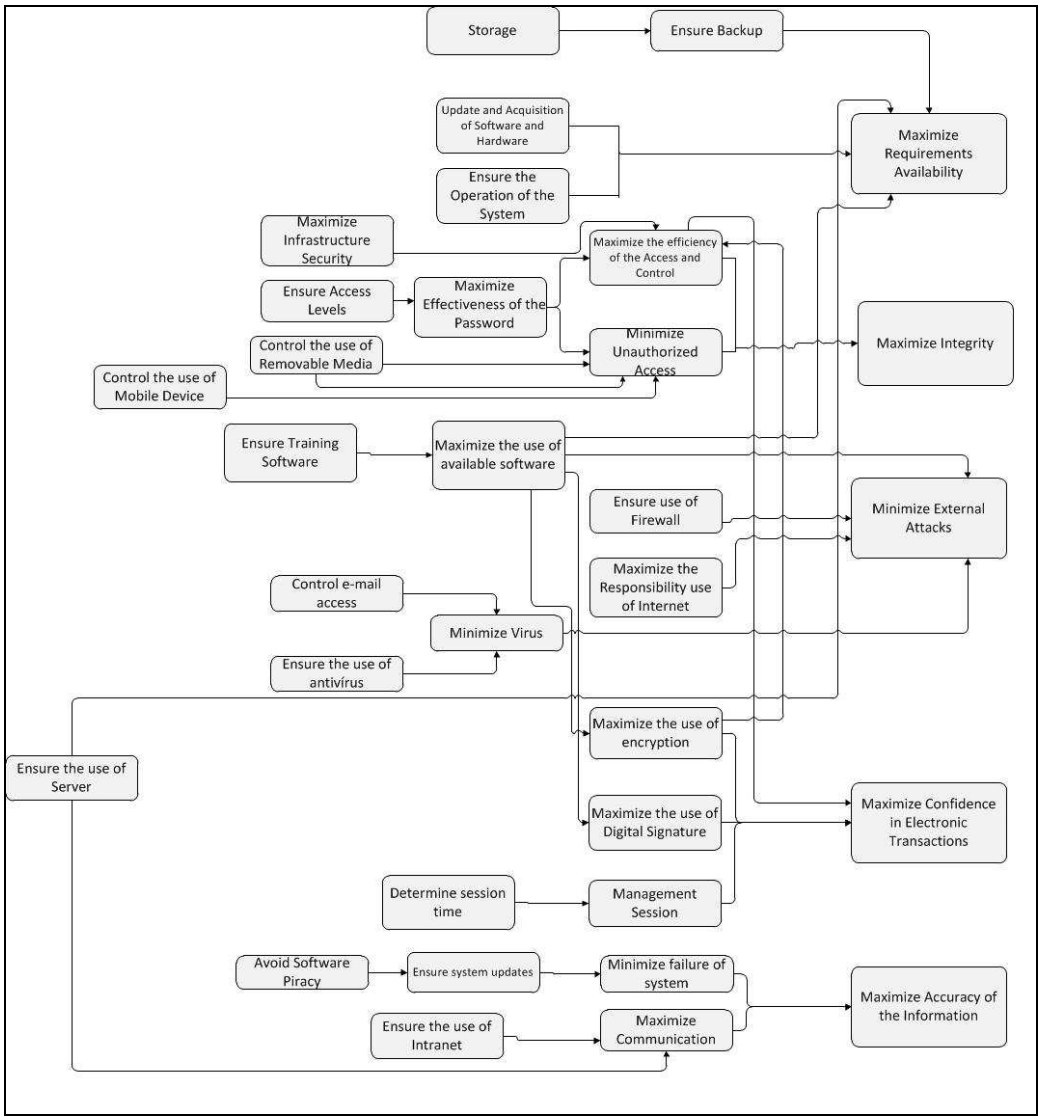

Figure 2. Structure of Objectives for Information Security Policies

Figure 2 shows that the main purpose of the specialists is to improve security in an organization. Also, this network will allow the stakeholders to guide how activities are planned and developed.

Therefore, to assess the degree of maturity of an organization in relation to its use of information security policies, this paper proposes the use of a percentage of IT security plans and policies developed and documented and communicated to all stakeholders in an organization.

Evaluation Framework

As mentioned before, the objective of this research is to combine the measures of the percentages of confidentiality, integrity, availability and non-repudiation that an organization has into a single measure that may be called the information security maturity model (ISMM).

These four measures have different priorities with respect to managing information security. Let X_C, X_I, X_A and X_N denote the percentage of policies that an organization currently has from all those described in Table 1, according to each factor.

The weighting factors could differ between organizations since confidentiality may well be more important than integrity for any one organization. Thus, each organization has to analyze for itself which weighting factor has most importance, and must define its value.

In this paper, in order to evaluate the ISMM, an additional set of four variables must be taken into consideration, namely: the Information Confidentiality Weighting Factor (ICWF), the Information Integrity Weighting Factor (IIWF), the Information Availability Weighting Factor (IAWF), and the Information Non-repudiation Weighting Factor (INWF), and it is required that:

$$ICWF + IIWF + IAWF + INRWF = 1 \quad (1)$$

Finally, the value of ISMM can be determined by aggregating the following four impacts: The combined impact of X_C and its weighting factor ICWF on ISMM, and so on.

The combined impact of X_C and ICWF on ISMM might be evaluated according to an additive model. In this case, it considers the value function $v_j(a)$ of each criterion to obtain the overall value function v(a). The following equation represents this model:

$$v(a) = \sum_{j=1}^{n} k_j v_j(a) \quad (2)$$

where, kj represents the weights for the criterion j, which is represented by ICWF, whereas vj(a) represents respectively the value of X_C, X_I, X_A and X_N.

As a final result, Table 4 presents an illustration of the global evaluation of the information security maturity model, based on Williams (2001).

Percentage	Level	Description
0% <= ISMM <= 20%	Very Low	The organization does not consider the impact associated with security vulnerabilities End users do not adhere to the Information Security Policy of the organization; this requires urgent intervention.
20% < ISMM <= 40%	Low	Security awareness is fragmented and limited. Security information is generated, but is not analysed.
40% < ISMM <= 60%	Medium	There is some level of adherence by end users to the Information Security policy of the organization but it is not satisfactory; constant monitoring and planning improvements are required.
60% < ISMM <=80%	High	Good level of adherence of end users to the Information Security Policy of the organization. IT security risk and impact analysis is consistently performed, but there are some minor gaps and lapses that need to be fixed.
80% < ISMM <= 100%	Very High	Security requirements are clearly defined, optimised and included in a verified security plan. Functions are integrated with applications at the design stage and end users are increasingly accountable for managing security

Table 2. Global Assessment of the level of compliance with Information Security Policy

CASE STUDY

The information security maturity model proposed was applied in companies in the health sector, to verify their level of maturity in information security.

The first case study was conducted in a public hospital, deemed Company A. It offers 33 specialties, and serves on average 12,000 patients per month. The hospital offers highly specialist services - such as: Cardiac Surgery, and Neurological and Renal Transplantation Units - to which patients from throughout the region are referred.

The second case study was conducted in a private hospital, deemed Company B, which is premised on providing treatment of constantly increasing quality, with the focus on patient safety and consolidating its leadership in the local market. This

includes a network of hospitals that is located in two states of the south-east of Brazil. The hospital also offers highly specialist services, such as clinical medicine, general surgery, cardiology, vascular surgery, neurology and neurosurgery, traumatology, hemodynamic, SOS burns, urology, gynecology/obstetrics, pediatrics and serves on average 10,000 patients per month.

In order to implement the model developed in this research, interviews with company managers were used. The conduct of the interviews focused on establishing a parallel between information security policies offered by the model proposed in this article with the security policies adopted by the company, as well as on investigating possible alternative or additional policies that might be adopted. This required seeking and receiving the support of the IT Manager in obtaining relevant information for this study. In the interview, the theme of "Information Security" was discussed taking into account the environment created by the public/private health sector and their respective measures for the safety of the information held in the hospital.

The following table summarizes all policies, based on this work, which are or are not adopted by each company. In this study, the same values were given to each weighting factor (ICWF = IIWF = IAWF = INRWF = 0.25).

Policies	Company A		Company B		Policies	Company A		Company B	
	Uses	Doesn't use	Uses	Doesn't use		Uses	Doesn't use	Uses	Doesn't use
PC_1		X		X	PA_1	X		X	
PC_2		X		X	PA_2	X		X	
PC_3	X		X		PA_3	X		X	
PC_4		X		X	PA_4	X		X	
PC_5	X		X		PA_5		X		X
PC_6	X		X		PA_6	X		X	
PC_7		X		X	PN_1		X	X	
PI_1		X	X		PN_2		X		X
PI_2	X		X		PN_3	X			X
PI_3	X		X		PN_4	X		X	
PI_4		X	X		PN_5		X		X
PI_5		X	X		PN_6	X		X	
PI_6	X		X		PN_7		X	X	
PI_7	X			X					
PI_8	X		X						
PI_9	X		X						

Table 3. Policies adopted by each company

From Table 3 and applying Equation 2, given that each factor has the same weight, since these factors were considered with equal importance, the following results were obtained: for the public hospital, a medium level of maturity, in accordance with the ISMM, which was 58.93%. On the other hand, the private hospital reached the high level of maturity, which was 68.05%.

The difference in the results of the ISMM enterprises the amount of information security policies adopted by each one. While the public company adopts 17 policies, the private one adopts 20, both being evaluated over 29 security policies.

CONCLUSION

Given the complexity of and the increasing threats to information systems, a growing emphasis has been placed on understanding the need to increase the number of information security policies in organizations

In the case study, the main objective was to analyze the information security policies that are used in public/private service companies and to understand what the current initiatives and future prospects are for implementing a new model of information security. Besides, this paper shows the application of SODA to structure this kind of problem.

As to the public hospital, this study was warmly accepted by the IT manager interviewed, because it is an important issue, which is not usually emphasized by the health public sector. Another point to note is the difficulty in specific investment for information security being made in the public sector. Since this study demonstrated the moderately unsatisfactory maturity level of the public hospital, it will be used by the IT Manager to seek new investment, since security deals with a variety of information that needs to be held under a measure of reliability that is high. The future perspective is to emphasize the security in integrity and the availability of computer systems and the infrastructure they require.

On the other hand, the private hospital accomplished a higher level of maturity. This may be because of its leadership in the local market. As a result, according to the IT Manager, its perspective is to adopt an outsourcing data center, with a view to minimizing the company´s responsibility for the possible loss of information.

Despite the contrast in the level of maturity between the two hospitals, it is not possible to affirm that private companies' maturity levels are higher than those of public companies, since the study was conducted in only two hospitals. However, this study does demonstrate that both companies, independent of the investments, have taken precautions with respect to attending to information security.

Finally, this paper presented a case study about the use of information security policies in a company in the public sector and another in the private sector. In addition, it presents a model, based on a multicriteria approach, which identifies the information security maturity level of an organization. Although there are as yet few information security policies, this model can be updated to include other policies as and when they are introduced and gain acceptance. Therefore, the model could calculate the best ISSM for an organization. It should be noted that, once a manager considers different weights factors, the value of the ISMM may vary.

It is noteworthy that there are government agencies that have other considerations in terms of security policies, including the tension that exists between the required disclosure of certain information and others that should not be freely available.

For further research, we suggest inserting more information security policies that should enforce the model and for its implementation to be replicated in other companies. Besides, we recommend the use of some methodologies to attribute the weighting factors under in a more formal procedure.

ACKNOWLEDGMENTS

This research is supported by the Brazilian National Council for Scientific and Technological Development (CNPq) to whom the authors are grateful. The authors are also grateful to the companies which took part in this study and in particular to their staff for making time available for the interviews.

REFERENCES

1. Ackermann, F., Eden, C. and Cropper, S.A. (1995) Getting started with cognitive mapping. Article supplied with Decision Explore software, Banxia Software, Glasgow.
2. Albrechtsen, E. and Hovden, J. (2010) Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study, *Computers & Security*, 29, 432–445.
3. Ayadi, I., Serhrouchni, A., Pujolle, G. and Simoni, N. (2011) HTTP Session Management: Architecture and Cookies Security, *Conference on Network and Information on Systems Security (SAR-SSI),* May 18-21, La Rochelle, France, pp.1-7.
4. Bacik, S. (2008) - Building an Effective Information Security Policy Architecture, CRC Press, FL.
5. Burke, B. E. and Christiansen, C. A. (2009) Insider risk management: a framework approach to internal security, IDC Analyze the Future, Sponsored by: RSA, The Security Division of EMC.
6. Byun, J. W. and Lee, D. H. (2011) On a security model of conjunctive keyword search over encrypted relational database, *The Journal of Systems and Software*, 84, 1364–1372.
7. Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, 24, 2, 84–88.
8. Chen, L. and Leneutre, J. (2011) Fight jamming with jamming – A game theoretic analysis of jamming attack in wireless networks and defense strategy, *Computer Networks*, 55, 2259–2270.
9. Chiong, R. and Dhakal, S. (2008) On the insecurity of personal firewall, IEEE.

10. Daniela, T. (2011) Communication security in SCADA pipeline monitoring systems, *RoEduNet 10th International Conference* (RoEduNet), June 23-25, pp.1-5.
11. DaRolt, J., Di Natale, G., Flottes, M.-L. and Rouzeyre, B. (2011) Scan Attacks and Countermeasures in Presence of Scan Response Compactors, *16th IEEE European Test Symposium (ETS),* May 23-27, Trondheim, Norway, pp.19-24.
12. Eden, C.; Ackermann, F. (1998) Making strategy: The Journey of Strategic Management. In: SAGE Publications, London
13. Faravelon, A., Verdier, C. and Front, A. (2011) Towards a business-centric definition of access control policies, *Fifth International Conference on Research Challenges in Information Science* (RCIS), May 19-21, Guadeloupe, France, pp.1-11.
14. Guzman, I.R., Galvez, S.M., Santon, J.M. and Stam, K.R. (2010) Information Security Practices in Latin America: The case of Bolivia. Americas Conference on Information Systems (AMCIS) Proceedings, paper 492. August 12-15, Lima, Peru.
15. Harn, L., and Ren, J. (2011) Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications, *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, July.
16. Jayadevappa, B. and Soh, B. (2009) A New Risk Analysis Method for Data Backup Strategy, IEEE TENCON.
17. Kayacık, H. G., Zincir-Heywood, A. N. and Heywood, M. I. (2010) Can a good offense be a good defense? Vulnerability testing of anomaly detectors through an artificial arms race, *Applied Soft Computing*, v. 11 4366–4383.
18. Kim, S.H. and Ahn, B.S. (1999) Interactive group decision making procedure under incomplete information. *Eur. J. Oper. Res*, 116, 498–507.
19. Knapp, K. J., Morris, R. F., Marshall, T. E. and Byrd, T. A. (2009). Information security policy: An organizational-level process model, *Computers & Security*, 28, 493–508.
20. Marciano, J. L. and Marques, M. L. (2006) O enfoque social da segurança da informação, Ci. Inf., Brasília, v. 35, n. 3, p. 89-98.
21. Matushima, R., Venturini, Y. R., Sakuragui, R. R. M., Carvalho, T. C. M. B., Ruggiero, W. V., Naslud, M. and Pourzandi, M. (2006) Multiple personal security domains, *Proceedings of the 2006 international conference on Wireless communications and mobile computing - IWCMC '06*, Vancouver, British Columbia, Canada, ACM Press, New York, USA , pp. Pages: 361 – 366.
22. McFadzean, E., Ezingeard, J. N. and Birchall, D. (2007) Perception of risk and the strategic impact of existing IT on information security strategy at board level, *Online Information Review*, 31, 5, pp. 622-60.
23. Moreira, E. S.; Martimiano, L. A. F., Brandão, A. J. S. and Bernardes, M. C. (2008) Ontologies for information security management and governance. *Information Management & Computer Security*, 16, 2, 150-165.
24. Pietro, R. Di, and Molva, R. (2011) An optimal probabilistic solution for information confinement, privacy, and security in RFID systems. *Journal of Network and Computer Applications*, 34, 853 –863.
25. Shirtz, D. and Elovici, Y. (2010) Optimizing investment decisions in selecting information security remedies. *Optimizing investment decisions*, 19, 2, 95-112.
26. Straub, D.W. (1990) Effective IS Security: an empirical study, *Information Systems Research*, 1, 3, pp. 255-276.
27. Tomono, A., Inutake, Y., Uehara, M., Shimada, Y. and Yamagiwa, M. (2010) VLSD based Backup System for Internal Control, *13th International Conference on Network-Based Information Systems*. September 14-16, Takayama, Japan.
28. Vasilyevna, N. B., Yeo, S., Cho, E. and Kim, J. (2008) Malware and Antivirus Deployment for Enterprise IT Security, *International Symposium on Ubiquitous Multimedia Computing*. October 13-15, Hobart, Australian.
29. Veiga, A. Da. and Eloff, J.H.P. (2010) A framework and assessment instrument for information security culture. *Computer & Security*, 29, 196–207.
30. Zhang, Q., Li, Z. and Song, C. (2011) The Improvement of digital signature algorithm based on elliptic curve cryptography, IEEE, 978-1-4577-0536-6/11.
31. Zhang, X. and Shuai, J. (2009) A New Feature Selection Method for Malcodes Detection, *Fifth International Conference on Information Assurance and Security*. August 18-20, Xi'an, China.

32. Zhongmeng, Z. and Hangtian, Y. (2010) A Data Backup Method Based on File System Filter Driver, *Second WRI World Congress on Software Engineering, IEEE.* December 19-20, Wuhan, China.
33. Yang, Y. O., Shieh, H.M. and Leu, J.D. (2009) A Vikor-Based Multiple Criteria Decision Method For Improving Information Security Risk, *International Journal of Information Technology & Decision Making*, 8, 2, 267–287.
34. Yayla, A. (2011) Controlling insider threats with information security policies. *Proceedings of the 19th European Conference on Information Systems* (ECIS), 242, Helsinki-Finland.
35. Yildirim, E. Y., Akalp, G., Aytac, S. and Bayram, N. (2011) Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey, *International Journal of Information Management* v.31 360–365.
36. Wei, C.H., Hwang, M.S. and Chin, A. Y. (2011) Mutual Authentication Protocol for RFID System, *IEEE International Conference on Computational Science and Engineering.* August 24-26, Dalian, China.
37. Williams, P. (2001). Information Security Governance. *Information Security Technical Report*, 6, 3, 60-70