A Business aware Information Security Risk Analysis Method

M. Sadok[1] and P. Spagnoletti[2]

Abstract Securing the organization critical information assets from sophisticated insider threats and outsider attacks is essential to ensure business continuity and efficiency. The information security risk management (ISRM) is the process that identifies the threats and vulnerabilities of an enterprise information system, evaluates the likelihood of their occurrence and estimates their potential business impact. It is a continuous process that allows cost effectiveness of implemented security controls and provides a dynamic set of tools to monitor the security level of the information system. However, the examination of existing practices of the enterprises reveals a poor effectiveness of information security management processes such as stated in the information security breaches surveys. In particular, the enterprises experience difficulties in assessing and managing their security risks, in implementing appropriate security controls, as well as in preventing security threats. The available ISRM models and frameworks mainly focus on the technical modules related to the development of security mitigation and prevention and do not pay much attention to the influence of business variables affecting the reliability of the provided solutions. This paper discusses the major business related factors for risk analysis and shows their interference in the ISRM process. These factors include the enterprise strategic environment, the organizational structure features, the customer relationship and the value chain configuration.

Introduction

Information is a valuable asset supporting management decisions and business operations within the enterprise. Consequently, securing the company critical information assets from sophisticated insider threats and outsider attacks is essential to ensure business continuity and compliance with regulatory frameworks. However, the evaluation of existing practices of the enterprises reveals a poor effectiveness of information security management processes such as stated in the information security breaches surveys. In particular, the 14th annual CSI re-

[1] Institute of Technology in Communications at Tunis, Techno park El Ghazala 2088 Ariana, Tunisia, moufida.sadok@gmail.com
[2] CeRSI – LUISS Guido Carli University, Via Alberoni 7, 00198 Roma, Italy, pspagnoletti@luiss.it

port [1] indicates increasing incidences, compared to the last year, of financial fraud, malware infection, denials of service, password sniffing, and Web site defacement. In the case of the UK businesses, the BERR ISBS report [2] reveals that although there is a wide consensus that security is a high priority to their board, only 55% have a security policy, 48% formally assess risks, 56% have procedures to log and respond to security incidents, 11% have implemented the ISO 27001 standard that provides a framework for information security management. In France, the CLUSIF report shows that only 55% of the interviewed enterprises have proceeded to the formalization of their security policy, 32% use ISO 17799 [3] to achieve this activity, only 30% carry out a total risks analysis related to their information system security and more than 75% of the companies do not measure their security level regularly.

These results indicate that the security controls and procedures established by the enterprises cannot match the requirements of their real business operations. We claim that reasons for this can be summarized as: (a) the enterprises experience difficulties in assessing and managing their security risks, in implementing appropriate security controls, as well as in preventing security threats; (b) the need to customize available ISRM frameworks to the business and the organizational context of the enterprise. In fact, some authors [4] have identified as a critical issue for the security managers the need to face both a set of predictable threats and a set of emerging and context related intractable problems. In the first case, a number of methods and techniques are available with the objective of reducing risks through the selection of appropriate countermeasures at a technical and procedural level. For the second class of problems, they introduce concepts such as formative context, improvisation and hacking to provide additional capabilities to the management. In the remaining part of this paper we will refer to the first category of threats, which require well structured and formalized techniques based on monitoring and control. Furthermore, recent works have emphasized the need for a holistic view on information security which takes into account both context related and behavioral aspects of organizational phenomena [5]. In fact each organization is subject to external regulations having an impact on security issues, such as for instance laws, regulations and agreements with other partners. Within this context, the ISRM is the process that identifies controls and minimizes security risks affecting information and business processes for an acceptable cost. It is the basis of effective governance and protection of the organization information assets [6]. It can be preceded by a risk analysis activity [7] that identifies the threats and vulnerabilities, evaluates the likelihood of their occurrence and estimates their potential business impact. There are many methodologies aimed at allowing risk analysis in order to help organizations assess their security risks and implement appropriate security controls. Despite the interest of these assessment methods, we have noticed that the organizational and managerial issues are insufficiently addressed and developed. These methods fail to estimate specific organizational and managerial parameters re-

lated to the security risk management. In fact, these methods remain mainly focused on the technical issues and factors related to the development of security protection. Many authors [8, 4, 5] argued that it is difficult to select an appropriate risk analysis method that will best suit the specific organization requirements. Several researches have highlighted the significant importance of management related risk analysis factors in the ISRM process, such as the changes of the internal and external environment of the organization [9], the business processes and internal controls [10], the business maturity that refers to the organization's position in the business lifecycle [11], the importance of various business functions and the necessity level of various assets [12], the cultural, and legislative issues [13]. Each organization is different in strategy, structure, resources and capabilities; therefore each will have specific information security requirements and risk management processes. Additional effort is needed to customize available ISRM frameworks to current or future business activities, organization and managerial procedures so as to ensure the cost effectiveness of implemented security controls. Thus, the objectives of this paper are firstly, to identify specific business related risk analysis factors; and secondly, to provide an enrichment of existing ISRM methods to address strategic, organizational and managerial issues. Our contributions in this paper are three-fold. First, we propose additional risk analysis factors according to a business view. Second, we discuss their interference with the technical processes of the ISRM. Finally, we provide an example of applicability of these factors within the NetRAM© framework which will be further introduced. The remainder of the paper is organized as follows. The first section reviews the most renowned risk management approaches and comments some shortcuts related to these methodologies. The second section shows how business and organizational parameters should be addressed. Section 3 presents an enhancement of NetRAM framework. Finally, the conclusion discusses perspectives for future researches.

Related works

The review of the common risk management frameworks reveals four mainly steps. They are (a) the classification of information assets according to their sensitivity, (b) the identification of the threats and vulnerabilities, (c) the likelihood occurrences and impact estimation of these threats and (d) the implementation of controls and corrective countermeasures taking into consideration their cost.

The research work of [14] and [15] provides an interesting report and evaluation of the most important standards (e.g. ISO 27001), guidelines (e.g. Risk Management Guide for Information Technology Systems [16]), and models (e.g. OCTAVE [17]) assessing and managing risks in the information security field. The authors high-

light mainly four weaknesses associated to the considered risk analysis approaches which are (a) the lack of cost estimation techniques related to risk management activities (b) the absence of techniques for scenario attacks reconstruction (c) the absence of relevant criteria to select appropriate control measures according to the enterprise specificities and (d) the lack of links between the business activity of the enterprise and the monitoring and security incident response during the risk management process. Consequently, the aforementioned authors have proposed a framework, called Network Risk Analysis Method (NetRAM©) based on ten modules, as illustrated by Figure 1. In this framework, the risk management is viewed as an iterative and learning process that allows adequate levels of reactivity and prevention through the possibility of the re-execution of risk management activities after the occurrence of new vulnerabilities or attacks threatening the enterprise information security. The NetRAM framework begins with an estimation of the cost and the planning of the different risk management activities. The objective of the asset analysis step is to collect data about information system components and to establish certain dependency links between them that might be useful for attack scenarios modeling. The processes of vulnerabilities and threats identification aim at classifying the weaknesses, the security breaches and the attacks that threaten valuable information assets. In the risk analysis process, the risks harming information assets are defined and ranked with regard to security needs. Then, based on the level of protection required for the analyzed information assets and the available budget, a set of security countermeasures is proposed, selected and implemented in the setting of a security policy. In the monitoring step, a set of relevant security metrics should be continuously measured and controlled to check periodically the information system operation and to maintain an acceptable security level. In the last process, decisions about security incident response are taken to select the most cost-effective reactions and to ensure the information system continuity.

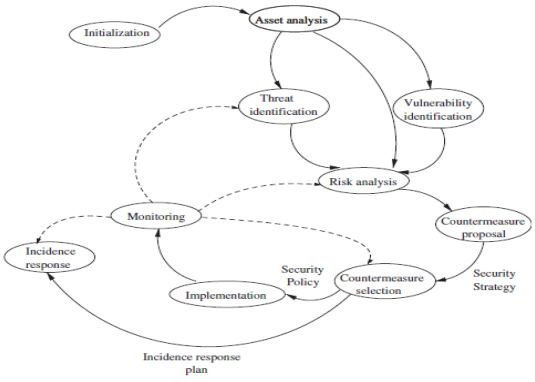

Fig. 1. The NetRAM framework for risk management [14]

In spite of the interest of NetRAM framework, only technical concerns are addressed. While NetRAM takes care of cost-benefit analysis and the management of security project development [18], it does not consider the enterprise business activities and the organizational procedures in the evaluation of risk analysis.

Business related factors for risk analysis

The ISRM process must reflect the organization's business activity and takes into account all aspects of how information is processed, stored and disposed. Due to the reality of nearly unlimited threats and the limited available security budget, critical decisions must be made concerning the implementation of protection and mitigation procedures to reduce the likelihood or impact associated with the security risks or the acceptance of risk that allow the business process to operate with a known risk under control. Cost-benefit analysis of risk mitigation and acceptance must be achieved to balance potential losses of integrity, confidentiality or availability of information resources against the expenditures on security countermeasures and controls. Furthermore, given the changing nature of technological and economic environment as well as the evolving risks, a dynamic and proactive risk management process capable of adapting company operational procedures, resource management, and corporate strategy to the evolution of security risks, is necessary. To this end, we propose four business related risk factors and show how they interfere in the NetRAM© framework. These factors involve the strategy, the organization, the customer relationship and the value chain configuration.

At the strategic level, we suggest to consider two parameters linked to the business environment of the enterprise. They are (a) the competition intensity and (b) the compliance with legal and governance frameworks. The former parameter indicates the competition pressure in the activity sector of the enterprise and highlights the need to protect the information system from economic intelligence. This parameter increases the vigilance of the enterprise that must be doubly careful and, affects the number of control points, the sophistication of security solutions and the regularity of monitoring activities. It also shows how damaging the threats targeting the enterprise activity can be. The legal and governance frameworks have increased the accountability and the liability of the corporate executives. If the enterprise adopts governance policies and procedures dealing with compliance with legal framework, the ISRM focuses on ensuring that the IT risks related to the business impact analysis are controlled and mitigated.

At the organizational level, the ISRM should integrate at least two parameters: (a) the level of procedure formalization and (b) the control system performance. The formalization of work processes through rules, procedures, and policy manuals improves the traceability of information processing and storage. It consequently facilitates the detection of incoherent management operations, manipulation errors or abuse. When the formalization level is low, the ambiguity within the organization increases the effort required to conduct risk analysis. Moreover, the existence of a well-organized control system reduces the errors related to either the decisions or the actions over a given period of time. Thus, also in this case the risk analysis process can be conducted more efficiently.

At the customer relationship level, the ISRM should integrate at least two parameters: a) the customer variety and b) the channel variety. The customer variety refers to the level of segmentation of customers that can lead to different kind of threats. The channel variety refers to the number of different channels available for providing the products/services.

Finally, there are two parameters associated with the value chain configuration. We refer to them as (a) the IT integration, and (b) the inter cyber process relations. The former parameter expresses the dependency level of the value chain on the use of IT for the operation of its activities. If this level is important, special focus must be placed on security solutions design in order to allow for more efficient value chain integrity. The second parameter describes the interfaces between the value chain processes. Control and visibility of the data flowing between processes should be protected against any harmful threat. The compliance of the rules governing the execution or management of these processes should be maintained any time a modification, an addition or a drop of rules is realized.

Towards a business-aware information security risk analysis

We find it convenient to include the aforementioned business related risk analysis factors to the different modules NetRAM framework[3]. Indeed, some among these modules cannot achieve their real objectives without considering the business related factors.

[3] Enhancement submitted to The Communication Networks and Security (CN&S) research Laboratory, at the University of 7th of November at Carthage for possible inclusion

The strategic environment affects considerably the security policy objectives that are an essential prerequisite for the initialization and asset analysis modules. According to the security policy, the organization classifies its information assets in accordance to their business value and sensitivity in order to ensure that effective protection takes place. The sensitivity is related to several environmental variables such as the security level required by the trading partners, the importance of the assets in the value chain operation, legal rules, and competitive pressure. These constraints increase the required level of confidentiality and integrity of business information, affecting the company reputation that is valued as an important asset. In the vulnerabilities identification module, special focus must be placed on organizational parameters. It is important at this stage to get well acquainted with operational procedures and the work methods employed to handle business information in order to identify the procedures, the practices and the personnel that could lead to a possible threat or vulnerability. During threats identification, the parameters related to the strategic environment of the enterprise have to be considered. In particular, the arrival of new competitors and the changes of the regulatory context can increase the probability of threats occurrence. Furthermore, in both the vulnerabilities and threats identification modules customer relationships parameters should be taken into account. For instance in case of a service provider, the number and the kind of threats and vulnerabilities vary with the number of customer interfaces (i.e. mobile, internet, call center, etc.). In the countermeasure management module, the selection of security controls is dependent upon organizational procedures, and should also be subject to all relevant legislations. The decision makers should set up the criteria for determining whether risks can be accepted according to the operational requirements and constraints of the business process activities. In this setting, the value chain configuration parameters should support such decisions to balance the investment between implementation and operation of the control thwarting the harm likely to result from security failures. In addition, the processes countermeasures should be integrated in the working practices, applied consistently across all operations, and should properly reflect the security policy guidelines. In the monitoring module, the internal and external levels of assets protection are evaluated. Through the surveillance of a set of important metrics and agent profiles, the monitoring module should be able to manage the state of the information system and should be capable of detecting operation anomalies and misuses. It is obvious that the definition of metrics, the estimation of the alarms levels, and the users' profiles are tightly related to the business factors, we have discussed. Finally, the decisions that would be made during the incident response module can have a direct impact on the formalization of certain organizational procedures and imposes new controls. It may generate new managerial controls or modify existing operational procedures. In particular, the cost, time and amount of modification should be evaluated for any decision to be selected. It seems consequently that NetRAM involves at the same level, security experts and decisions makers. Indeed, close collabora-

tion between business unit operators and technical staff (e.g. security incident team) is necessary with the purpose of responding to business needs in terms of sharing information, defining sensitivity levels and discussing effectiveness of protection procedures.

Conclusion

The research aim of this paper was to determine a set of business related information security risk analysis factors. More specifically, one objective was to identify strategic and organizational parameters and determine the extent to which these parameters affect the ISRM process. Another objective was to provide a generic ISRM model to the managers in order to assist critical decisions in information security activities and to meet the changing business needs of their organizations. It is necessary to recognize that some risk analysis factors may not be applicable to every information system or environment, and might not be relevant for all organizations. Future research aiming to collect data related to the risk analysis for various types of organizations and business activities would help in gaining better adjustment of the proposed ISRM model.

References

1. 2009 CSI Computer Crime and Security Survey. Computer Security Institute, available at: http://www.gocsi.com/.
2. 2008 Information security breaches survey, available at: www.security-survey.gov.uk.
3. Iso/iec 17799:2000 (part 1), Information technology-code of practice for information security management.
4. Spagnoletti P., Resca A. (2008), *The duality of Information Security Management: fighting against predictable and unpredictable threats*, Journal of Information Systems Security, Vol. 4 - Issue 3, 2008
5. Åhlfeldt R.M., Spagnoletti P. and Sindre G. (2007) *Improving the Information Security Model by using TFI*. In "New Approaches for Security, Privacy and Trust in Complex Environments", IFIP Springer Series, Springer Boston, Volume 232/2007, 73-84
6. Humphreys, E. (2008) Information security management standards: Compliance, governance and risk management, *Information security technical report* 13: 247–255.
7. Bandyopadhyay, K., P. P. Mykytyn and K. Mykytyn (1999) A framework for integrated risk management in information technology, *Management Decision* 37(5):437-444.
8. Eloff, J., L. Labuschagne and K. P. Badenhorst (1993) A comparative framework for risk analysis methods, *Computers & Security* 12: 597-603.

9. Tchankova, L. (2002) Risk identification - basic stage in risk management, *Environmental Management and Health* 13(3): 290-297.
10. Finne, T. (2000) Information Systems Risk Management: Key Concepts and Business Processes, *Computers & Security* 19: 234-242.
11. Broderick, J. S. (2001) Information Security Risk Management –When Should It be Managed?, *Information Security Technical Report* 6 (3) : 12-18.
12. Suh, B. and I. Han (2003) The IS risk analysis based on a business model, *Information & Management* 41: 149–158.
13. Gerber, M. and R. von Solms (2005) Management of risk in the information age, *Computers & Security* 24, 16-30.
14. Hamdi M. and N. Boudriga (2005) Computer and network security risk management: Theory, challenges, and countermeasures, *International journal of communication systems* 18:763–793.
15. Krichene, J. (2008) Managing Security Projects in Telecommunication Networks Ph.D. Thesis Engineering School of Communications, SUP'COM.
16. Stonebumer, G., A. Grogen, and A. Fering, Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology. Special publication 800-830.
17. Alberts C. and A. Dorofee (2002) *Managing Information Security Risks: The OCTAVE Approach* Addison Wesley Professional.
18. Krichene, J. and N. Boudriga (2007) Network security project management: A security policy-based approach, *in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, (SMC 2007) Montréal, Canada October 7-10.