An Ontology Approach in Designing Security Information Systems to Support Organizational Security Risk Knowledge

Teresa Pereira[1] and Henrique Santos[2]
[1]*Polytechnic Institute of Viana do Castelo, Viana do Castelo, Portugal*
[2]*University of Minho, School of Engineering, Department of Information Systems, Guimarães, Portugal*

Keywords: Information Security, Information Systems Security, Information Security Risk Management, Ontology, ISO/IEC 27001.

Abstract: Organizations increasingly demand faster and flexible operations promoted by information and communication technologies, particularly on the Internet and the newer technologies, such as the internet-enabled services, mobile and wireless devices and networks, with a complete disregard of their security vulnerabilities and underestimating risks that this new technologies impose. A proper information security risk management is difficult and becomes crucial to ensure the daily operational activities of organizations as well as to promote competition and to create new business opportunities. Moreover there is a lack of formal and flexible models to support a proper information security risk management process. This paper presents an ontology developed in the security domain aimed to support organizations to deal with huge security information issues and therefore implement a proper management to facilitate the decision-making regarding their security needs.

1 INTRODUCTION

Organizations heavily rely their activity on the performance of their information systems. Besides their information systems, organizations rapidly adopt new services based on Internet, mobile and wireless devices, with complete disregard of their vulnerabilities and their risks' exposition. With security mechanisms adopted such as firewalls, IDS, IPS et cetera, organizations have to deal every day with new security information that needs to be properly managed. The security standards ISO/IEC and NIST are an important reference in the security information domain. However, most of the security experts follow their own interpretation of the standards, according to their experience and their perceptions about security, which certainly leaves overlooked flaws in the organization information system security. This fact has imposed new demands and challenges to the information security risk management process, evidencing a serious problem of lack of knowledge about the practical solutions to implement in order to objectively improve security within an organization. In fact, it is observed that each organization follows its own approach to security management, resulting sometimes in misusing concepts, implementation of improper controls and even in unbalanced risk assessment.

In this context, it is proposed an ontology approach based on a conceptual model defined according to the security standard ISO/IEC 27001, with flexible capability, which enable its adoption by any organization, regardless their business activity, to support their information security risk management process.

The paper is structured as follows: in section 2 it is presented an overview of information security management. In section 3 it is presented an approach to the security risk analysis. In section 4 it is presented an example of a security risk assessment method, OCTAVE. In section 5 it is presented the ontology developed and conclusions will be presented in section 6.

2 INFORMATION SECURITY MANAGEMENT

Managing information security in particular the information systems security is increasingly concerning organizations, due to the continuous

Pereira T. and Santos H..
An Ontology Approach in Designing Security Information Systems to Support Organizational Security Risk Knowledge.
DOI: 10.5220/0004180004610466
In *Proceedings of the International Conference on Knowledge Engineering and Ontology Development* (SSEO-2012), pages 461-466
ISBN: 978-989-8565-30-3

growing dependence of organizations on technologies to conduct their businesses, to create a competitive advantage and achieving higher ROI. Organizations must consider how they are going to succeed to the continuous changing risk environment, since the technical controls mechanisms alone are no longer guaranteed, but mainly dependent on other security requirements such as legislation, culture or environment (Onwubiko and Lenaghan, 2009). Recognized organizations such as ENISA (European Network and Information Security Agency) and OECD (Organization for Economic Cooperation and Development) are making strong efforts to promote a culture of security, focusing in the development of information systems security and improve security communications and the adoption of new ways of thinking and behaving by all participants when using information systems and communicating technologies.

According to ENISA and OECD raising information awareness is the first and huge challenge to any organization (OECD, 2009). Organizations need to evolve security management strategies according to the evolvement of information security management strategies in response to emerge of new information security requirements. A properly security strategy demands for a rigorous process, where every agent interacting with critical resources need to be aware and participate in security management, both adopting secure behaviours and continuous evaluating security control's performance (CCMB, 2006).

The Information Security Management Systems (ISMS) is a concept introduced in the security standard ISO/IEC 27000 and provides a model, named PDCA (Plan-Do-Check-Act), to establish, implement, operate, monitor, review, maintain and improve the protection of information assets, which are critical to the operational activity of the organization and requires adequate protection against the loss of relevant properties such as confidentiality, integrity and availability, to achieve business objectives based on a risk assessment and risk acceptance levels of the organization, designed to effectively deal with and manage risks (ISO/IEC, 2009). In other words, the ISMS reflects the organization's approach to risk assessment and risk management, the level of risk that an organization is willing to accept and the controls to be implemented. An adequate information security risk management process requires a security planning in order to collect information for awareness, followed by the implementation of the necessary mechanism required in a risk analysis process.

In following section it will be introduced an overview of the information security risk analysis.

3 SECURITY RISK ANALYSIS

Information security risks analysis is an integral part of information security management activities and consists in the systematic use of information to identify sources and to estimate risks (ISO/IEC_JTC1, 2008). This activity is especially important when the organization heavily depends on IT-based systems to remain viable. These decisions are performed based on the cost-benefit evaluation of applying controls and assessments of acceptable risk of the secured systems.

In all organizations, regardless of their business activity, the security risk management process should comprise the following actions:

- Identification of critical assets of the organization;
- Investigation of the vulnerabilities inherent to the assets;
- Identification of threats the assets;
- Evaluation of the implemented controls;
- Identification of the impacts that losses of confidentiality, integrity and availability may have on the assets.

The identification of the assets should address a substantial level of detail in order to provide enough information for the risk assessment. The result should be a list of assets to be risk-managed, and a list of business process related to the assets and their importance (or value) to the organization.

The threats identification results from incident reviewing and surveying users, as well as other sources including external threat references. The collected information will enable to produce a list of threats with identification of threat type and source.

The investigated vulnerabilities consist in finding the assets' weaknesses, which can be exploited by a threat. The vulnerabilities should be continually monitored and reviewed. Concerning information technologies there are a lot of automatic scanning tools, which are good in discovering known vulnerabilities. However, concerning new technologies and in particularly the human interaction and misbehaviour (a very important source of vulnerabilities), a lot of specific and reflexive work needs to be done.

The identification of implemented controls intends to evaluate the organization defence capacity, analysing if the controls putted in practice

are working correctly and know exactly what is protected. A special analysis should be considered when a selected control or a strategy fails in operation and therefore an auditing is required to find fails causes. A procedure to estimate the effect of the control is through the analysis of how the control reduces a threat.

An incident impact consists in the analysis of the consequences that an attack has over an asset and the global loss it imposes to the organization. A security incident can address a loss of effectiveness, adverse operating conditions, business loss, reputation and physical damage. An incident can affect one or more assets or part of an asset. Therefore assets should have assigned both financial cost values and business impact values.

Nevertheless, many organizations do not follow these actions. Actually, it is observed that organizations mainly follow their own security risk management practices. Some of them more focused on the efficiency of their controls, disregarding the critical assets of organizations. Others are exclusively focused on asset's value, which can result in either over-securing or under-securing assets (Hoo, 2002). Others estimate a value to the risk by enumerating all assets including their value and determining all the threats to them, estimating the impacts of the threats (Ekelhart et al., 2009).

Nevertheless, organizations that started implementing these approaches are taking the first step to improve their corporate information security.

In the next section will be presented an overview of the OCTAVE approach, which is not a formal model, but a method to support the security risk assessment process.

4 OCTAVE A SECURITY RISK ASSESSMENT APPROACH

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) was developed by SEI (Software Engineering Institute), Carnegie Mellon University, and includes a set of tools and techniques for risk based information security strategic assessment and planning (Alberts and Dorofee, 2001).

The OCTAVE focuses on organizational risk and strategic management and settles operation risk and security practices. It defines a set of self-directed activities to enable organizations to identify and manage their information security risks. This means that OCTAVE follows a workshop-based approach that requires the participation of staff members from key operational areas from both business department and information technology department, since information security includes also both business and technology related issues. The final goal is to provide a global understanding with different perspectives about the organizational view of the information security risk. This way it is assured that the evaluation is scoped properly, that the organization's senior managers participate in the evaluation, and that everyone participating in the process understands his or her role promoting responsible behaviour and awareness.

The involvement of persons from different business departments, proposed in OCTAVE approach is the main strategy followed by this method, contributing to promote awareness and compliance with best practices. However OCTAVE is mostly used by a few numbers of organizations, especially larger organizations than medium and small organizations.

Despite the aforementioned aspects, OCTAVE presents some issues, which not play a favourable role in the security risk analysis process. Namely:

- it requires a long process and thus too time consuming;
- it demands experts on the key areas of the organization, with skills to identify assets, vulnerabilities, threats as well as security policies and practices to support the decision-making. Furthermore, most organizations don't have those key experts from different organizational levels with knowledge to identify all the security information, which in turn imposes limitations to a continuous and reliable risk evaluation;
- OCTAVE does not promote a formal model, which makes it harder to get normalization or generalization. This is one of the greatest battles of ENISA and OECD organizations that are developing efforts to achieve a formal model in order to reduce the ad-hoc approach to security risk analysis process that is followed by most organizations.

In the following section will be presented the ontology defined.

5 THE ONTOLOGY DEVELOPED

The ontology developed represents the conceptual model derived from the established security standard ISO/IEC_JTC1 (International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), Joint Technical Committee (JTC

1)), and its application to some supporting tools (Santos, 2006).

The purpose of the developed ontology is to establish a conceptual model to structure information by introducing semantics, in order to enable organizations to firm up and unify the concepts and terminology defined in information security domain, based on the ISO/IEC_JTC1. The establishment of those concepts and their relationships enables to perform an effective security risk analysis and consequently improves information security management within organizations. Through the conceptual model each organization should be able to respond to the following action items: (1) properly identify the valuable or critical assets; (2) properly identify the vulnerabilities of assets; (3) identify and mitigate potential threats; (4) evaluate the risks; (5) evaluate the efficiency and effectiveness of the countermeasures defined and therefore analyse and implement the necessary adjustments to the security policy adopted. Such understanding can assist organizations in implementing the right combination of protection controls to mitigate security risks related with asset's vulnerabilities. An ontology approach with capabilities to jointly model all the integrated concepts and their relationships to other security concepts stands an important advance, challenging the information systems security management process.

The defined conceptual model comprises 8 concepts and 16 relationships, based on the security standards ISO/IEC_JCT1 and are represented in the ontology structure, as illustrated in Fig. 1.

These concepts are described as following:

Incident – A single or series of unwanted or unexpected events that might have significant probability to compromise the information system security.

(Security) Event – An identified occurrence of a particular set of circumstances that changed the status of the information system security.

Asset – Any resource that has value and importance to the owner of the organization, which includes information, programs, network and communications infra-structures, software, operating systems, data and people.

CIA – The information properties to be ensured, namely: confidentiality, integrity and availability; besides these main security properties, and depending on the context, other security properties may need to the addressed, such as: authenticity, accountability and reliability.

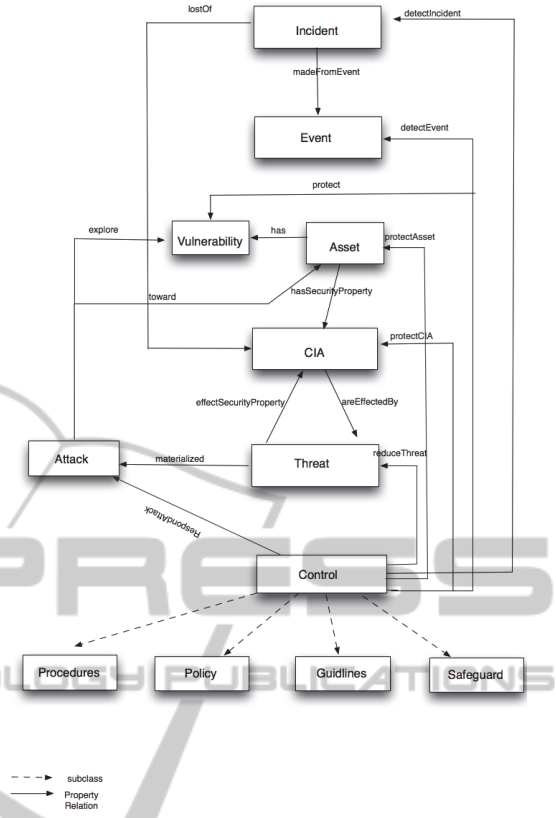

Figure 1: Concepts and relationships defined in the conceptual model.

Threat – Represents the types of dangers against a given set of properties (security properties). The attributes defined in this concept follow the Pfleeger approach (Pfleeger *et al,* 2007), which include an attacker actions or position to perform an interception, fabrication, modification and interruption, over a resource.

Attack – A sequence of actions executed by some agent (automatic or manual) that explore any vulnerability and produce one or more security events. Instances of this concept are based on the Bishop taxonomy to classify attacks (Bishop 2004).

Control – A mechanisms used to detect an incident or an event, to protect an asset and their security properties, to reduce a threat and to detect or prevent the effects of an attack. Instances of this concept are based on the ISO/IEC FDIS 27001:2005(E) (ISO/IEC_JTC1 2008).

Vulnerability – Represents any weakness of the system. Instances of this concept are based on the vulnerability taxonomy provided by the CVE (Common Vulnerabilities Exposures).

The use of taxonomies facilitates the identification of different instances of each concept

and even more important is that establish relations between concepts, which enables to infer information from those relations. These taxonomies were selected since they are an important reference in the security domain.

The rationale behind the ontology is structured as follows: an incident is made from – *madeFromEvent*- one or more events; the occurrence of an incident can lead to a loss of - *lostOf* - a set of security properties (CIA); an asset has security properties - *hasSecurityProperties* - and each one can be affected by a threat; on the other hand, a threat can *affectSecurityProperty* one or more security properties; and finally, an asset *has* vulnerabilities. A threat is *materialized* into an attack, while the attacks *exploit* one or more vulnerabilities; an attack is also triggered *towards* an asset. Furthermore, the implementation of control mechanisms helps to *reduce* threats, to *respond* an attack, to *protect* security properties; to *protect* assets and vulnerabilities, as well to *detect* events, in order to *protect* assets.

All these concepts and their relationships were formalized through the use of the W3C standard language for modelling ontologies Web Ontology Language (OWL). This web language has been developed by the Web Ontology Working Group as a part of the W3C Semantic Web Activity (Smith *et al,* 2004). This language was selected because it is a W3C recommendation since February of 2004 and due to its expressiveness with superior machine interpretability. The OWL vocabulary is an extension of RDF and uses RDF/XML syntax. The formalization of this ontology in OWL is a step forward to promote its interoperability among different information security systems.

6 CONCLUSIONS

The use of ontologies in the information security management process is a solution to succeed, since they clearly enable to define, classify and link the related concepts and relations shared by the community and formally defined. Several authors have indicated that security community needs ontologies (Donner, 2003) (Tsoumas *et al*, 2006) and they have considered this need as an important challenge and a research branch (Blanco *et al,* 2007).

The conceptual model based on the security standards ISO/IEC 27001, formally represents security concepts and their relationships in terms of threats, attacks, vulnerabilities and countermeasures.

Apart from promoting the standardization of the concepts defined in the information security domain, the simplicity and flexibility of the model, enables its adoption by any organization, regardless, their business activity, but embedding its own view and assumed risk exposition. It also contributes organizations to evolve their security information according to their needs, without having to redo the information. This is possible since one of the main features of the ontologies is the ability to create a dynamic, structured and formal knowledge base. Additionally, the relationships established between concepts allow the security experts to have different perspectives about security in a consistent and structured way. Managing all these information can assist organizations in implementing the right combination of protection controls to mitigate security risks related with the asset's vulnerabilities, providing an overall view of the organization security business activity and making the decision-process much more accurate.

Finally the formalization of the ontology in OWL is an important resource to promote its interoperability among different information security systems, as well as its integration in other knowledge representation system in the security domain.

ACKNOWLEDGEMENTS

This work was funded by FEDER through Programa Operacional Fatores de Competitividade – COMPETE, and by national founds through FCT – Fundação para a Ciência e Tecnologia, under project: FCOMP-01-0124-FEDER-022674.References

REFERENCES

Alberts, C., Dorofee, A., Managing Information Security Risks: *The OCTAVE (SM) Approach*. 1st ed. Addison Wesley.

Bishop, M., 2004. *Introduction to Computer Security*. 2nd ed. Addison-Wesley Professional.

Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R., Toval, A. "Basis for an integrated security ontology according to a systematic review of existing proposals", *Computer Standards & Interfaces*, 33 (4), 2007, pp. 372-388.

Common criteria for information technology security evaluation, Part I: introduction and general model, version 3.1, revision 1, CCMB-2006-09-001, September 2006.

Donner, M. “Toward a security ontology”. *IEEE Computer Society*, 1(3), 2003, pp. 6–7.

Ekelhart, A., Fenz, S., Neubauer, T. “Ontology-based decision support for information security risk management”, In: R. Ege, W. Quattrociocchi, D. Dragomirescu, O. Dini, eds. Proc. The Fourth *International Conference on Systems (ICONS 2009),* Gosier, Guadeloupe/France. IEEE Computer Society, 1-6 March 2009, pp. 80–85.

Hoo, K. J. S. “How much is enough? A risk-management approach to computer security”, *Workshop on Economics and Information Security*, 16-17 May 2002 University of California, Berkeley.

ISO/IEC, 2009. ISO/IEC 2nd WD 27002 (revision) - Information technology - Security techniques – Code of practice for information security management. ISO copyright office: Geneva, Switzerland.

ISO/IEC_JTC1, 2008. ISO/IEC FDIS 27005 Information Technology - Security Techniques - *Information Security Risk Management*. ISO copyright office: Geneva, Switzerland.

Onwubiko, C., Lenaghan, A. P. “Challenges and complexities of managing information security”, *International Journal of Electronic Security and Digital Forensics,* 2(3), 2009, pp. 306–321.

OECD, OECD Guidelines for the security of information systems and networks: *Towards a culture of security*. 2002, Paris.

Pfleeger, C., Shari, L. *Security in Computing*, 4th ed. Prentice Hall PTR, 2007.

Santos, H. ISO/IEC 27001. *A norma das norma em Segurança da informação*, 2006.

Smith, M. K., Welty, C., McGuinness, D. L., “*OWL Web Ontology Language Guide. W3C Recommendation 10 February 2004*” [on-line], W3C, 2004. Available from: http://www.w3.org/TR/owl-guide/. [Accessed 20 May 2010].

Tsoumas, B. and Gritzalis, D. “Towards an Ontology-based security management”. Proc. 20th International Conference on Advanced Information Networking and Applications*, IEEE Computer Society*, 18-20 April 2006 Vienna. Vienna University of Technology.