ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

An Ontological Approach to Information Security Management

Harshal A. Karande

P.G Student, Dept. of Computer Engineering, Siddhant College of Engineering, Savitribai Phule University, Pune, India

ABSTRACT: Information Security Risk Management is gathering significant attention in organisations today. Incident response teams are set up to handle cyber incidents. Adequate security procedures to manage information security are obviously required and organizations need to carefully evaluate their security policies. In this context information security risk management should be performed as part of information security management activity. Its objectives are to identify, address, and mitigate risks before they become serious threats. The definition of an ontology, which contains a hierarchical representation and description of security concepts, defined according to the ISO/IEC_JTC1 standards, can assist organizations to classify attacks, identify the critical assets and mitigate their vulnerabilities and threats. With this information organizations are able to identify the level of risk exposition. This paper proposes a method based on an ontological approach to structure and organize security information within an organization.

KEYWORDS: Information security management, Risk analysis, Security risk management, Information security, IT security, Ontology

I. INTRODUCTION

The increasing use of information technology brings significant risks to organizational information systems and particularly to the critical resources, due to its own nature. An increasing number of sophisticated attacks are expected to evolve as wireless, mobile and others technologies transcend local and secure utilization. This fact enforces the need to adjust security practices to manage organizational information security. It becomes crucial to organizations to adopt a proper security management approach in order to be able to identify their needs regarding information security requirements and to create an effective information security management system (ISMS). This approach should be suitable for the organizational environment, and in particular it should be aligned with overall enterprise risk management balancing flexibility with security. Risk management should be an integral part of all information security management activities and should be applied both to the implementation and the ongoing operation of ISMS (ISO/IEC_JTC1 2008).

This paper intends to present an investigated approach to support information security risk management through a conceptual framework developed to assist organizations to classify attacks, identify assets and mitigate their vulnerabilities and threats. The proposed framework is based on a conceptual model with capability to represent concepts and their relationships, defined according to the established security standards ISO/IEC_JTC1 (ISO/IEC_JTC1 2005).

The paper is structured as follows: in section 2 an overview of security risk management will be presented; in section 3 we briefly introduce the related work, which includes the presentation of the most widely used risk frameworks; section 4 presents the proposed conceptual model, containing the semantic concepts specified in the information security domain, and their relationships, hierarchical structured in an ontology; section 5 demonstrates the proposed framework to support security risk management, based on the information structured in the ontology; and finally conclusions and future work are presented in section 6.

DOI: 10.15680/IJIRCCE.2015. 0309026

II. SECURITY RISK MANAGEMENT

According to the security standard ISO/IEC FDIS 27001:2005(E) risk management coordinates activities to direct and control an organization with regard to risk (ISO/IEC_JTC1 2005). Additionally risk analysis should be performed as a part of risk management process and consists in the systematic use of information to identify sources and to estimate the risk (ISO/IEC_JTC1 2005). A set of security strategies to deal with risk and to support the decision -making on acceptable risk levels are investigated. The strategies consist in the implementation of security policy options, which can produce different effects on risk, such as mitigation of risk. At the end, an acceptable risk level is determined and a plan for achieving that point is adopted. Additionally the cost-benefit evaluation and assessment of acceptable risk which is usually involved in this decision-making process, is performed.

The identification of risks comprises the following issues (ISO/IEC_JTC1 2005):

- Identification of the critical assets of the organization.
- Investigation of the vulnerabilities inherent to the assets.
- Analysis of the threats to those assets.
- Examination 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 attacks. The vulnerabilities should be continually monitored and reviewed. The identification of implemented controls intends to evaluate the organization defense capacity, analyzing if the controls put in practice are working correctly and exactly what is being 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 failure causes. A procedure to estimate the effect of the control is defined 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.

All these issues should be reviewed and monitored in order to enable the identification of any changes in the context of the organization and to maintain some sort of risk indicate value. The ongoing monitoring and review should be performed in a continuous basis in order to improve as necessary and appropriate the operating security controls. Moreover, it is needed to assure that no risk is overlooked or underestimated, that necessary actions are taken and decisions made to provide realistic understanding and ability to respond accordingly.

III. RELATED WORK

Over the years, several security risk approaches have been developed with different features but with similar purpose: (a) to support managers to perform adequate security risk management, (b) to respond to the technology and environment evolution that brings underestimated and unexpected threats. Currently there are some security risk approaches and security methodologies developed by recognized standard organizations and recommended by ENISA[1] to support the risk management process, such as those provided by NIST, ISACA and ISO. NIST developed a framework named OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) process which is a risk management method from Carnegie Mellon University. OCTAVE defines components of a systematic context-driven information security risk evaluation (Alberts & Dorofee 2001). The use of the OCTAVE method by an organization enables to take security information decisions based on risk analysis. OCTAVE follows a three-phase

DOI: 10.15680/IJIRCCE.2015. 0309026

approach, which enables to have a comprehensive view of the information security needs of the organization. The OCTAVE phases are (Alberts & Dorofee 2001):

Phase1: Build Asset-Based Threat Profiles – Key areas of expertise within the organization are examined to identify important information assets, the threats inherent to the assets, the security requirements of the assets, the mechanisms the organization is currently practicing to protect its assets (protection strategy practices) and weaknesses in organizational policies and practice (organizational vulnerabilities).

Phase2: Identify Infrastructure Vulnerabilities – In this phase the key operational components of the technology infrastructure are examined, in order to find weaknesses (technology vulnerabilities) that can lead to security events.

Phase3: Develop Security Strategy and Plans – The information generated by the organizational and infrastructure evaluations performed in phase 1 and 2 are analyzed to identify risks to the enterprise and to evaluate the risks based on their impact to the organization's objectives. In addition a security strategy is developed, including mitigation plans addressing the highest priority risks.

Another security risk approach frequently used is ISACA's risk IT, part of COBIT. Risk assessment in COBIT goes beyond security risks. It includes development, business continuity and other types of operational risks related to IT. The COBIT's approach to risk management is very limited, since the risk is estimated through the result of not implementing an objective control and the value of the control. In the COBIT approach the primary risk to be managed is the accomplishment of the objectives. The identification of assets and their weaknesses are not covered as well as the impact analysis of a security incident. In the COBIT approach the risk assessment is only based on the overall set of IT objectives. Moreover it is a solution that uses the same methodology to all organizations, regardless of their business activity. Notwithstanding it is evident that each organization has its own security requirements accordingly to its business activity and financial goals and the COBIT approach is too wide which makes its adoption very difficult and complex. AURUM derived from *Automated Risk and Utility Management* and it is also a framework developed for information security risk management. AURUM allows automated information security risk management, including objective measures of risk and risk reduction by taking the entire setting of the organization into account (Ekelhart et al. 2009). This framework is based on an ontology defined in the information security domain, to ensure that information security knowledge is provided in a consistent and comprehensive way to the risk manager. The information represented in the ontology involves the concepts threat, vulnerability and controls, which is limited when compared to the ontological approach proposed in this paper. The standard ISO 27005 is part of the ISO 27000 series that includes ISO 27001 and ISO 27002 with the knowledge concepts, models, processes and terminologies. The general concepts specified in ISO/IEC 27001 are defined to support the implementation of information security based on a risk management approach. The ISO/IEC 27005 is not considered a security framework but a rather a methodology with guidelines to support the information security risk management. ISO 27005 follows a similar structure to that proposed by NIST but comprises different phases. The ISO 27005 includes more steps, namely context establishment, risk assessment (which includes the identification of threats, vulnerabilities and analysis of controls), risk treatment, risk acceptance, risk communication and risk monitoring and review. The ISO standards provide a good method for formal risk The OCTAVE is a formal and detailed set of processes, and will assist in ensuring that risks are identified and properly analysed, following the standard techniques used in most risk analysis procedures. However, due to the level of activity and overhead involved in OCTAVE, it is probably best suited for large organizations or projects.

This is merely an overview of the widely available security approaches. Our goal is to provide a general idea of the type of frameworks available, and their relative relevance and application. At this stage it is evident that no security framework is suitable for all applications. Different frameworks provide multiple perspectives and consequently different views of (the same) security. Information security is a transversal area resulting in a very complex topic, prone to various interpretations of similar activities and concepts, which gives space to several equivalent methods and tools. Besides this diversity, complexity typically leads to time consuming and difficult to understand tasks explored by private companies and offered, sometimes, as an unnecessary complex security solution. To address this issue, the proposed model, based on an ontology structure, brings relevant improvements to the security risk management process, since the proposed conceptual model leads to normalization and consequently can speed the process by reducing the learning curve and promoting sharing capabilities.

IV. THE PROPOSED ONTOLOGY

The methodology proposed to perform analyzes to information security management risk is based on a conceptual model, which contains security concepts hierarchally represented in an ontology. The adoption of an ontology structure was considered to be an appropriate strategy to organize and structure the fundamental terminology and concepts involved in the security information domain. The defined concepts are based on widely recognized standard, produced by ISO/IEC_JTC1.

The study of attacks, threats and the assets' vulnerabilities in an information system continues to grow because it is evolving and has significant impacts on an organization. Managing those concepts requires both a detailed understanding of security concepts and their relationships. Such understanding can assist organizations in implementing the right combination of protection controls to mitigate security risks related with the assets' vulnerabilities. The implementation of a conceptual model, richly represent security concepts and their relationships in terms of threats, attacks, vulnerabilities, assets and countermeasures (Onwubiko & Lenaghan 2007). The advantages of this approach to organizations are that it enables them to: (1) properly identify the valued 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 security policies and safeguards defined and therefore analyze and implement the necessary adjustments to security policy adopted.

Figure 1 illustrates the proposed framework, based on conceptual ontology with capabilities to join model attacks, threats and vulnerabilities resources, and their relationships to other security concepts, remains an important advance in managing information systems security. The defined conceptual model comprises 8 concepts and 16 relationships, based on the security standards ISO/IEC_JCT1 and was represented in an ontology structure.

These concepts are described as follows:

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 infrastructures, 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 be addressed, such as: authenticity, accountability and reliability.

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 & Shari 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.

Control – A mechanism used to detect an incident or an event, to protect an asset and its security properties, to reduce a threat and to detect or prevent the effects of an attack.

Vulnerability – Represents any weakness of the system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

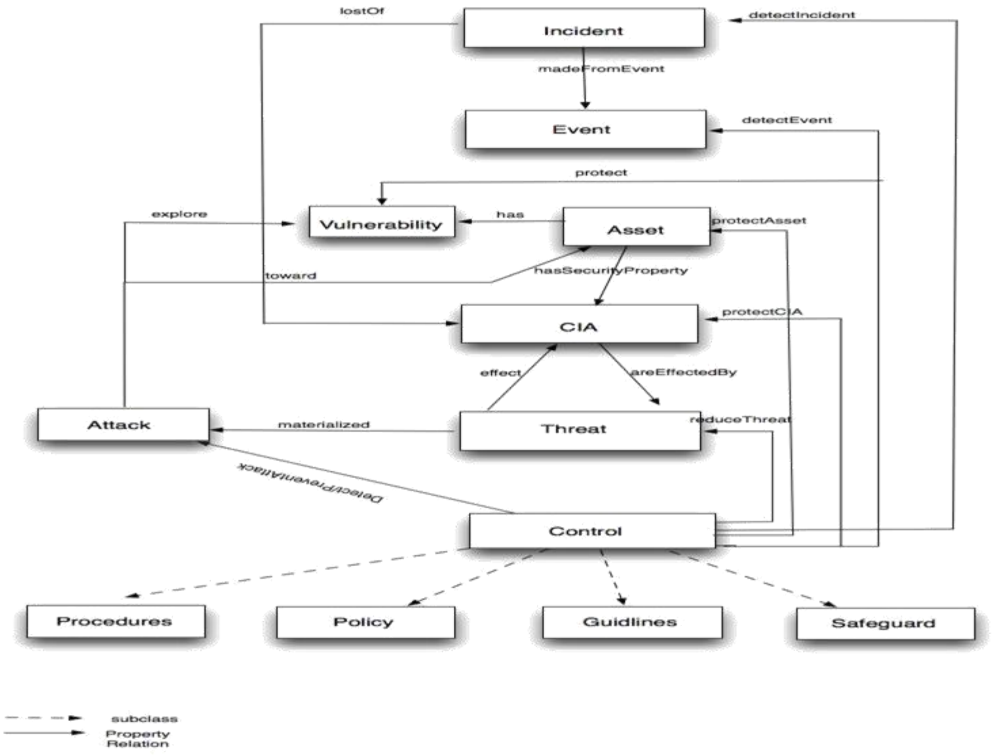

Figure 1: Concepts and relationships defined in the conceptual framework

In short, the rationality behind the ontology is structured as follows: an incident is made from –*madeFromEvent*- events; the occurrence of an event can lead to a lost of - *lost Of* - 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 *affect* one or more security properties; and finally, an asset *has* vulnerabilities. A threat is *materialized* by an attack, while the attacks *exploit* one or more vulnerabilities, an attack is also triggered *towards* an asset. Furthermore, the implementation of control mechanisms, help to *reduce* threats, to *detect* and *prevent* an attack, to *protect* security properties; to *protect* assets and vulnerabilities, as well as to *detect* events, in order to protect assets (Pereira & Santos 2009).

The description of those concepts and their relationships, presented in the ontology, was formalized through the use of the W3C standard language for modeling ontologies Web Ontology Language (OWL). This web language has been developed by the Web Ontology Working Group as part of the W3C Semantic Web Activity (Smith et al. 2004). Although OWL has not been designed to specifically express security issues, it was selected because it is a W3C recommendation since February of 2004 and due to its expressiveness with superior machine interpretability. The OWL is build upon Resource Description Framework (RDF) and Resource Description Framework Schema (RDFS). In fact the OWL vocabulary is an extension of RDF and uses RDF/XML syntax. The formalization of this ontology in OWL will be a step forward to promote its interoperability among different information security systems.In the next section, we will be presented the framework under proposal, which follows the hierarchical structure of the semantic concepts represented in the defined ontology, and try to provide an easy way to understand the risk magnitude that organizations have to face. Additionally it serves as a guide to identify the assets' vulnerabilities or control weaknesses that allow the exploitation of a threat and/or the materialization of an attack.

V. DEVELOPED FRAMEWORK

The establishment of ISO/IEC_JTC1 standards promoted the standardization of the concepts defined in the information security domain. The correct understanding and identification of those concepts are the primary requirements to be considered in the performance of a proper risk management analysis. The concepts structured in the ontology provide a mean to identify and characterize an occurred security incident, as well as to estimate its impacts. Within a security incident it is important to determine the assets, which were compromised, the vulnerability exploited and the controls that failed. The identification of the vulnerability exploited enables to determine the threat that may have been materialized in the attack. Finally, the evaluation of the controls implemented in order to perform the adequate adjustments to the security control to prevent or mitigate future attacks and threats.

VI. CONCLUSION AND FUTURE WORK

The formal, methodical risk analysis concerns the organizations about the magnitude of business risk according to the value of their information systems. The organization needs to have an overall knowledge of their business activities and be aware of the risks they have to face. Additionally risk can be managed or reduced when managers are aware of the full range of controls available and implement the most effective controls.

The contribution in this paper is a proposed framework based on a conceptual model approach to support the manager to primarily understand the business requirements in managing security of an organization, through the (1) identification of the critical assets of an organization; (2) identification and assessment of the vulnerabilities in the assets; (3) identification of the potential threats that might be materialized in attacks; (4) evaluation of the risks; (5) finally, assessment or reassessment of the policy and controls adopted. This solution compared to the currently available frameworks introduces a new perspective to model security information. In fact, a framework based on a conceptual model with capabilities to richly describe multiple security resources within an organization is an important advance compared to the current frameworks that specifically address restricted security issues. Besides the aforementioned advantage of this framework, it is pertinent to highlight that it also promotes firming up and unifying the concepts and terminology defined in the scope of information security, based on the relevant ISO/IEC_JTC1 standards. Furthermore, it enables the organization to evolve its own instantiation of the security ontology, obeying to standard concepts, but embedding its own view and assumed risk exposition. As future work we intend to evaluate the usability of the framework developed in organizations.

REFERENCES

1. Alberts, C. & Dorofee, A., 2001. An Introduction to the OCTAVE Method. Available at: http://www.cert.org/octave/methodintro.html.
2. 2.E., R. & JR., M., 2011. Sizing Up Risk. *Information Security*, 13(2), pp.28-35.
3. Ekelhart, A., Fenz, S. & Neubauer, T., 2009. Ontology-Based Decision Support for Information Security Risk Management. Em *Fourth International Conference on Systems, 2009. ICONS '09*. Fourth International Conference on Systems, 2009. ICONS '09. IEEE, pp 80-85.
4. ISO/IEC_JTC1, 2005. *ISO/IEC FDIS 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements,* Geneva, Switzerland.: ISO copyright office.
5. ISO/IEC_JTC1, 2008. *ISO/IEC FDIS 27005 Information Technology - Security Techniques - Information Security Risk Management,* Geneva, Switzerland.: ISO copyright office.
6. 6.Onwubiko, C. & Lenaghan, A.P., 2007. Managing security threats and vulnerabilities for small to medium enterprises. In Intelligence and Security Informatics, 2007 IEEE. p 244–249.
7. Pereira, T. & Santos, H., 2009. An Ontology Based Approach to Information Security. *In Communications in Computer and Information Science, Metadata and Semantic Research, Part2. Communications in Computer and Information Science. Third International Conference, Metadata and Semantic Research (MTSR)*. SpringerLink, p 183–192. Available at: http://www.springerlink.com/content/t28h080v74636530/.
8. Pfleeger, C. & Shari, L., 2007. *Security in Computing* 4th ed., Prentice Hall PTR.
9. Smith, M.K., Welty, C. & McGuinness, D.L., 2004. *OWL Web Ontology Language Guide.* W3C Recommendation 10 February 2004., Available at: http://www.w3.org/TR/owl-guide/.

BIOGRAPHY

Mr. Harshal Ashokrao Karande, he received the B. Tech (2008) degree in Computer Science & Engineering from "Department of Technology", Shivaji University, Kolhapur (Maharashtra). He is currently pursuing M.E in Computer Engineering from "Siddhant College of Engineering", Savitribai Phule University Pune, Pune(Maharashtra), India.

DOI: 10.15680/IJIRCCE.2015. 0309026