Security Management and Knowledge Engineering

Nucharee Premchaiswadi
Faculty of Information Technology, Dhurakij Pundit University
110/1-4 Prachachuen Road, Laksi, Bangkok 10210, Thailand
nucharee@dpu.ac.th

Abstract

This paper presents a security management using knowledge management. It appears that knowledge engineering and knowledge management could be of help to organizations for security risk management, identifying security threats, identifying threat countermeasures effectiveness, and frustrating potential security adversaries by establishing an ontology model for information security and creating software to use the ontology model based on knowledge engineering and knowledge management practices. Moreover, it is possible with an ontology model to create a simulation using information system entities and threat relationships to expose areas of weakness for potential information security threats.

Keywords: security management, knowledge engineering, information security.

1. Introduction

Information security is critical to organizations as well as individuals since it allows them to assure the properties that make their information useful, including confidentiality, authenticity, integrity, and availability. For many organizations in the internet based world, information is a critical commodity. The various pieces of information used by these organizations are referred to as their *information assets*. Some of these assets are internal, proprietary information that may not be easily reversible if removed, corrupted, or blocked from the organizations' use. Other assets are information on external entities including identifying information of customers, business partners, government organizations, as well as payment-processing information, or records of transactions that have taken place. This information is maintained as custodial property by the organization without which no effective or legitimate transaction can be executed, and use of this information is typically restricted by the agreement under which the information was provided. Forrester Research [7], in a survey of over 300 corporations, found that this custodial data had a mean value of $750,000 per organization. In contrast, the executives of these firms placed more than double this value on the internal information used in the operation of these corporations, including:

- logistics and production information,
- business plans and
- new product forecasts,
- earnings and
- financial info,
- employee information,
- proprietary research and
- Clinical trials, etc.

It can be seen that the information technology and security also has crucial functions in both society and business as well [8][9].

2. The Value of Information

The value placed on information often is not derived based on the cost of gathering or generating the information. In some cases, organizations spend significant resources gathering or generating information, and then ultimately give the information away for free for marketing, customer support, reputation building, image creation, or participation in professional societies, among other reasons. Instead of the initial investment; the value comes from the use the organization makes of the information. That use is partially determined by the properties of the information, and the protections associated with those properties. For information to be useful it must have a reliable meaning. This meaning must be protected by assuring the information's data integrity preventing undesirable and unauthorized changes to the information. By protecting information integrity, an organization assures that the content, format, and semantics of the information remain controlled by the organization, facilitating continued reliable use. The information must provide an advantage for its use, providing a benefit not available to everyone. This advantage may derive from the information's confidentiality by restricting the knowledge of the information to authorized parties. By protecting confidentiality, the organization retains control over which parties have access (or use of the information), restricting competitors from exploiting this information. The information must have legal authority for its use. This authority is assured by the authenticity of the information protected by non-repudiation, which is the ability to definitively identify the source of the information. By protecting authenticity, the organization assures a trace from the responsible individuals to any actions performed on or with the information. The information must also be accessible when needed by the organization. The accessibility is assured by availability protections, which are provisions to ensure that the information and its processing capabilities are providing service as designed whenever users make authorized requests. Protecting availability involves ensuring the presence of the information, its access rights, usable formatting, and suitable computing resources for processing the information.

While all of these characteristics of information are required for use in organizations as well as by individuals, the importance of each characteristic varies from organization to organization. In financial institutions, data integrity is paramount because if an institution loses the reliability of its information, regulators will shut it down. In e-businesses, availability is the key issue since loss of service may lead to large losses of revenue. For many military and police applications, confidentiality is the most important property – disclosure to the enemy of military plans or operations could be fatal to the personnel involved. In each of these situations, the value of the information and therefore, the value of an organization is increased via the protection of the information and decreased by lack of such protection.

3. Information Security Measures

Information security systems are used as measures that implement services that attempt to assure adequate protection for information systems used by or hosted within an organization. In this definition, “services” are technical or managerial methods used with respect to the information being protected, and “information systems” are computer systems or communication systems that handle the information being protected. However, the term“ protection” implies the combination of integrity, confidentiality, authenticity, and availability. Information security violations arise when an *actor* takes advantage of vulnerabilities in a system that processes information. An *actor*, in this sense, is some entity, person or process that serves as a root cause for the violation. Vulnerability is a flaw in the system including its daily operation and management practices that can be exploited to violate the system’s security policy and practices. Vulnerabilities can be introduced throughout a system’s life-cycle.

There are several assumptions made by the adversaries also known as hackers. One assumption is that any executable portion of a system could be used to break it, whether or not it is executed on a frequent basis. Another assumption is that the actors/adversaries may deliberately choose to use inputs to the system that are the opposite of the specified inputs (by length or by content) in order to break its security. Most system developers are focused on making the system functionally correct and minimizing errors, comparatively few know how to make a system secure. Other developers know how to make a system secure but fail to include security in their concept or design for their systems. The result is that there is much vulnerability in deployed information systems, particularly networked information systems.

Vulnerabilities in information systems are discovered in several different ways. Users may accidentally identify vulnerabilities in the course of their authorized use of the information system. Competitors sometimes find vulnerabilities in competing products. Security firms may identify vulnerabilities using detailed analysis of source code or using system-level testing techniques. Vulnerability is a potential security violation which is basically a doorway that can be entered to violate an organization's security policy. An exploit is a process that uses a vulnerability to violate security policy via vulnerability. Most exploits are developed after the associated vulnerabilities are known and described; sometimes even after a fix for the vulnerability has been published. Some system developers will only fix vulnerabilities when they have identified exploits for those vulnerabilities. On current computer networks, most exploits are implemented as computer software or program fragments to be used within computer software. This malicious software, frequently abbreviated as *malware*, may not necessarily be developed by agents intending to violate the security of organizations, but rather may be developed for profit (e.g. by selling it to the affected vendors or to those intending to violate security) or to provide a clear demonstration of vulnerabilities so that they may be fixed. Much malware is developed by those intending to use it to violate security for profit purposes.

4. Security Control Approaches

There are two complementary approaches that have helped organizations to effectively apply multiple controls namely: Security Risk Management and Security Strategies. Security Risk Management is any process of identifying, measuring, and mitigating potential loss of information security so as to reduce the expectation of such loss to a level acceptable to the organization. Security strategies as described by Shimall and Spring [1] take a number of different approaches. An initial strategic approach is deception which includes either fooling the malicious actors as to where to direct their activity or fooling them with respect to the degree of success of their activity. A second strategy is frustration which is making the initial penetration into the organization as difficult as possible. A third strategy technique is resistance, where activity following the initial penetration is hampered as much as is reasonable and the final strategy is an integrated recognition and recovery process from the activity of the malicious actors. These strategies can work together to allow improved mitigation of modern threats and their potential impact.

5. Using Knowledge Engineering to Aid in Information Security Solutions

The preceding has provided some information security principles and a definition for some of the common terms in this field. These principles aid in the management of information security risks. As the malicious actors in this field have become better resourced and more persistent, simple defensive controls have become less effective [1]. Currently Security Managers are mainly focused on the management and interpretative techniques to help decision-makers, governments, security consultants and researchers to correctly evaluate the massive amounts of data generated by security controls. The analysis of this massive and complex data is extremely difficult, but essential to achieve new discoveries and make efficient business decisions. Knowledge Engineering provides a basis for researchers and practitioners to discuss practical challenges encountered and solutions adopted in the scope of Information Security Intelligence and all related issues.

Knowledge engineering refers to the development of systems that use knowledge, rather than simply data, to solve many unique computing problems. This is achieved by the application of computing techniques, closely associated with human cognitive processes, for transforming data into knowledge. It is possible to enhance security of information systems through the development of an architecture sustaining knowledge of Information Technology security within an organization. This architecture would use a tailored set of security processes, policies and solutions to protect the organization's business. The proposed architecture would need to capture the organization’s security-related knowledge in order to share it and transfer it throughout the organization. The purpose would be to increase the efficiency of handling security incidents and to minimize the dependency on security expert personnel. Unified and formal knowledge models of the information security domain are a fundamental requirement for supporting and enhancing existing risk management approaches. Such a knowledge model could be used to support a broad range of information security risk management approaches. Incomplete knowledge about the information security domain in general and the current information security status of an organization is one of the main problems in information security risk management.

Knowledge engineering can be used to create and manage ontologies to sort the security information (messages, protocols, algorithms, threats) in a coherent and consistent way, closer to the human thinking process. This knowledge can then be used to create methods to identify threat weaknesses, deceive, frustrate, resist and recognize /recover from attacks by adversaries. This knowledge architecture could be based on

- Analyzed risk management approaches,
- Existing literature, and
- Risk management requirements,

6. Using an Ontology Model

As we mentioned earlier, an ontology model [4] that is comprised of the concepts of threat, vulnerability, and control to represent the information security domain knowledge needs to be constructed. Besides these core concepts, concepts and relationships necessary to formally describe the organization and its assets would have to be incorporated into the model. While a formal description of the core concepts may have to be based on interpretive research, the formal description of the non-core concepts could also rely on already existing taxonomies such as the United Nations Standard Products and Services Code. The analyzed information security knowledge sources have to be mapped to the security ontology model. To enrich the knowledge model with concrete information security knowledge an analysis of several best-practice guide-lines and information security standards regarding their acceptance, completeness, availability, and knowledge representation have to be made. Also a security manual such as the German IT Grundschutz Manual, (considered the best security manual) or a similar manual could be superimposed on the security ontology Information security concepts and corresponding formal axioms could be integrated into the ontological knowledge base. The main challenges at the knowledge integration level are the differences regarding knowledge models and the knowledge granularity of manuals and guidelines like the German IT Grundschutz Manual. With such a knowledge model available, organizations would not only have a formal reference representation to understand which controls have to be implemented to fulfill specific security standards, but also have automated reasoning about the current organization's security status, based on the organizational model. With such a knowledge model available, organizations would not only have a formal reference representation to understand which controls have to be implemented to fulfill specific security standards, but would also have automated reasoning about the current organization's security status, based on the organizational model [5].

Singhania University [6] has proposed a model to improve information security using knowledge management techniques. The model mainly has three modules namely as:

- Information security knowledge repository module,
- Information security knowledge sharing and dissemination module, and
- Information security knowledge implementation & effectiveness module.

The Information security knowledge repository module stores the information security knowledge in a systematic and easy to use format. The Information security knowledge sharing and dissemination module promotes sharing and disseminating the security knowledge, and the Information security knowledge implementation and effectiveness module is responsible for monitoring and measuring the effectiveness of the total information system.

7. Ontology Model Components

The components of an ontology model [3] for information security are shown below:

System Components:

Hardware - PCs, Servers, Printers,
Hubs, Routers Switchboards,
Gateways, etc.

Software - Operating System, System
Software utilities, Loaders, Device
Drivers, Programming tools, application
Software

Platforms - Physical Platform, Network
Physical Network, Virtual Network

Users – IT personnel, Organizational
Personnel, Customers, Vendors

Asset Components:

Data (databases, Files, etc.)

Environmental Components:

Location, Site, Building, Floor, Passage
Room

Service Components:

Power Supplies, Communication Links, etc.

Security Components:

Threats

Threat Type

Environmental Threats

Fire, Flood, etc.

Personnel Threat

Insider Attack, vendor attack

Network Threat

Intrusion Attack, etc.

Physical Threat

Equipment Failure

Equipement/Data Theft

Threat Tree

Defense

Countermeasure

Threat Countermeasure

8. Ontology Model Relationships

Once the ontology components/entities have been identified and defined, the relationships among the components/entities and the potential threats must be defined. These relationships are shown below:

Relationships

Threat-Entity Relationship (TE)

ThreatEntity-ThreatEntity Relationship (TETE)

ThreatEntity-Countermeasure Relationship (TEC)

IncidentTETECountermeasureResidualTETE Relationship (TETE-C-TETE)

Entity-Entity Relationship (EE)

Asset-Platform Relationship

Asset-Application Relationship

After this model has been defined, it will be possible to build a computerized model such as the one proposed by Shuangyan Liu, Chinghang Cheung and Lamfor Kwok in the Department of Computer Science, City University of Hong Kong [2] as shown below in Fig. 1.

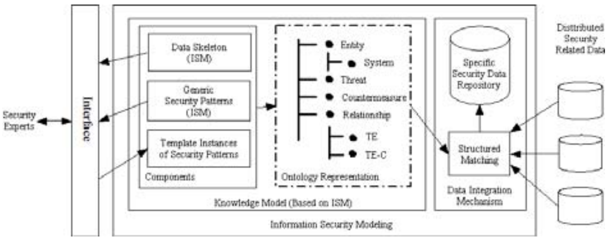
Security Experts
Interface
Data Skeleton (ISM)
Generic Security Patterns (ISM)
Template Instances of Security Patterns
Components
Entity
System
Threat
Countermeasure
Relationship
TE
TE-C
Ontology Representation
Knowledge Model (Based on ISM)
Specific Security Data Repository
Structured Matching
Data Integration Mechanism
Information Security Modeling
Distributed Security Related Data

Fig. 1. A Knowledge Framework for Information Security Modeling

Using such a model it will be possible to write a risk simulation which can help security officers to obtain an entire set of impacted entities specific to an organization in case a threat happens. Such a simulation includes the following tasks:

(1) Identify threats to an organization;

(2) Demonstrate the outcome of a threat acting on one entity or multiple entities.

These tasks have complex requirements for the data collection process, which includes preparation of threat profiles, and formal definitions and aggregation of impacted entities within an organization. The ontology model can act as a basis for the simulation or other automated aids for protecting the security of information held by organizations.

9. Conclusion

As more and more organizations and individuals utilize the Internet with applications that require revealing personal information, cyber-criminals and other adversaries will attempt to steal information and disrupt systems. These adversaries day by day have become more highly resourced and better skilled which places information security at a higher risk than ever before. The typical defensive measures for ensuring the security of information are no longer an adequate level of protection. Therefore, knowledge engineering and knowledge management could be of help to organizations for security risk management, identifying security threats, identifying threat countermeasures effectiveness, and frustrating potential security adversaries by establishing an ontology model for information security and creating software based on the knowledge engineering and knowledge management practices. Yet, it is possible with an ontology model to create a simulation using information system entities and threat relationships to expose areas of weakness for potential information security threats.

References

[1] Timothy Shimeall and Johathan Spring. Introduction to Information Security, 1st Edition; A Strategic-Based Approach. Elsevier, 2013.

[2] Shuangyan Liu, Chinghang Cheung and Lamfor Kwok in the Department of Computer Science, City University of Hong Kong. Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

[3] Anderson A, Kwok L F and Longley D. Security Modelling for Organizaitons. Proceedings of 2nd ACM Conference on Computer and Communication Security. Fairfax Virginia, USA, 24, November, 1994, pp.241- 250.

[4] Benjamins, R., Fensel, D. and Gomez Perez A. Knowledge Management through Ontologies. In U. Reimer (editor), Proceedings of the Second International

Conference on Practical Aspects of Knowledge Management. 29-30 October, 1998, Basel, Switzerland.

[5] Kwok L F. A Hypertext Information Security Model for Organizations, Information Management and Computer Security, Vol. 5, No. 4, 1997, pp.138148.

[6] Yogesh Kumar Mittal1, Dr Santanu Roy2 and Dr. Manu Saxena3, A Knowledge Management Model to Improve Information Security. IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, November 2010 ISSN (Online): 1694-0814

[7] Forrester Research. The Value of Corporate Secrets: How Compliance and Collaboration Affect Enterprise Perceptions of Risk, March 2010

[8] N. Premchaiswadi, The impact of information technology on Society and Business, Engineering Journal of Siam University, Vol.13, Issue 1, No.24, pp.50-67. 2012.

[9] N. Premchaiswadi, Intelligent system and society, Engineering Journal of Siam University, Vol.14, Issue 1, No.26, pp.71-82. 2013.