

Challenges of Web-based Information Security Knowledge Sharing

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

im Rahmen des Studiums

Information & Knowledge Management

eingereicht von

Daniel Feledi

Matrikelnummer 0426231

an der

Fakultät für Informatik der Technischen Universität Wien

Betreuung

Betreuer/in: O.Univ.Prof. Dipl.-Ing. Dr.techn. A Min Tjoa

Mitwirkung: Dipl.-Ing. Mag. Dr. techn. Stefan Fenz

Wien, _____.____.____

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Kurzfassung

Heutzutage nehmen Informationssysteme eine sehr wichtige Rolle für Organisationen und Individuen ein, weshalb ihr Schutz einen immer größeren Stellenwert einnimmt. Häufig werden Lösungen für sehr ähnliche Informationssicherheitsprobleme immer wieder aufs Neue entwickelt. Hier wäre ein Wissensaustausch zwischen Experten wünschenswert damit nicht ständig dieselben Lösungen von unabhängigen Personen erarbeitet und somit wertvolle Ressourcen verschwendet werden. Ein solcher Austausch könnte auch zu qualitativ hochwertigeren Lösungen führen, da bestehende Lösungsansätze weiterentwickelt werden könnten, statt immer neue zu entwickeln.

Diese Diplomarbeit hat zum Ziel, ein bestehendes Webportal für IT-Sicherheitsexperten zu erweitern, um die Erfassung und den Austausch von Wissen zu erleichtern.

Im Anschluss an die praktische Entwicklungsarbeit wurde eine Evaluierung des Webportals mit Sicherheitsexperten durchgeführt, um die Funktionalität und die Usability zu untersuchen.

Neben diesen Erweiterungen am bestehenden System wird der derzeitige Stand der Forschung auf diesem Gebiet erfasst um zu klären, auf welche Art und Weise sich Wissen zwischen Organisationen austauschen lässt und wie ein Tool den Wissensaustausch unterstützen kann.

Die Forschungsergebnisse zeigen, dass ein Wissensaustausch an konkrete Anreize gekoppelt sein muss, um Teilnehmer entsprechend zu motivieren. Diese Anreize können ökonomischer Natur sein (z.B. Kostenersparnisse) oder aber auf der Erwartung basieren, dass für das Einbringen des eigenen Wissens zumindest gleichwertige Information erhalten wird. Zusätzlich muss eine Vertrauensbasis aufgebaut werden, ohne die ein Austausch nur sehr begrenzt möglich ist.

In Bezug auf die Unterstützungsmöglichkeiten durch ein Tool waren die wesentlichen Ergebnisse, dass ein kollaboratives Tool für Experten sowohl als Nachschlagewerk als auch im Bereich der Risikoanalyse brauchbar wäre, allerdings unter der Voraussetzung, dass eine vertrauenswürdige Umgebung geschaffen wird. Wichtig ist in diesem Zusammenhang auch die "kritische Masse" an Inhalten, welche erreicht werden muss, damit das Tool für neue Nutzer interessant wird.

Bisher gibt es kaum technische Lösungen für den Wissensaustausch, weshalb der in dieser Arbeit präsentierte Ansatz durchaus weiter verfolgt werden sollte.

Die Evaluierung hat ergeben, dass die Umsetzung nützlich sein kann, allerdings wurden auch zahlreiche Herausforderungen identifiziert. So muss in der weiteren Entwicklung ein stärkerer Fokus auf die finale Zielgruppe gerichtet werden, damit speziell für diese Gruppe ein Mehrwert entwickelt werden kann. Durch die Entwicklung weiterer Anreize könnten dann gezielt Experten angelockt und motiviert werden, damit sie ihr Wissen mit Anderen teilen.

Abstract

Nowadays information systems play a vital role for organizations and individuals, which is why their protection is becoming increasingly important. Often, solutions are developed for very similar problems over and over again. An exchange of knowledge between experts would be desirable in order to prevent developing always the same solutions by independent persons. Such an exchange could also lead to solutions of higher quality, as existing approaches could be advanced, instead of always reinventing the security wheel.

This thesis aims to extend an existing web portal for IT security experts to facilitate the collection and sharing of information security knowledge.

Following the practical development work, an evaluation of the web portal has been conducted with security experts to examine the functionality and usability.

In addition to these enhancements to the existing system, the present state of research in this field is captured, in order to determine in what way knowledge can be shared between organizations and how a tool can support this exchange of knowledge.

The exploration of these questions showed that an exchange of knowledge must be linked to concrete incentives, in order to motivate participants accordingly. These incentives can be of economic nature (e.g. cost savings) or can base on the expectation that through contributing own knowledge, one receives information of at least equal value in return. In addition, trust has to be developed between the participants to facilitate knowledge exchange.

Concerning the question of how a tool can support the knowledge exchange, the results showed that a collaborative tool can be useful as a reference work for experts as well as in the field of risk analysis, but under the condition of being placed within a trusted environment and / or community. It could also be shown that a "critical mass" of content must be reached so that the tool will be of interest to new users.

There is still much space for developing technical solutions for information security knowledge sharing. The web portal presented in this master thesis represents one approach to offer a collaborative platform for knowledge sharing.

Though the approach is useful, several challenges could be pointed out. In the process of further developing the web portal, it is important to put a stronger focus on determining the final target group. This will help to concentrate on the needs of this group and to develop a unique selling point, making the web portal more attractive to use. At the same time incentives have to be developed to attract experts and to motivate them to contribute their knowledge.

Table of Contents

1	Introduction.....	6
1.1	Importance of knowledge	8
1.2	Influence of human behavior	10
2	Sharing information security knowledge	15
2.1	Managing information security knowledge within organizations.....	15
2.2	Sharing information security knowledge between organizations	31
2.3	Conclusion	53
3	The security ontology web portal	54
3.1	The security ontology	54
3.2	Extending the security ontology web portal	60
3.3	Implementing the security ontology web portal extensions	64
4	Evaluation of the security ontology web portal	86
4.1	Assignments	86
4.2	Questionnaire: Impressions and opinions.....	88
4.3	Analysis of collected data	89
4.4	Assessment of the analysis.....	95
4.5	Outlook and future work.....	98
5	Conclusion	101
5.1	Outlook	105
6	References.....	107

1 Introduction

Nowadays many organizations and companies rely heavily on information systems and have to ensure that they work properly at any given time. Additionally *"Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures form a vital part of [...] economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures."*¹ Often they are part of critical information infrastructures where *"their disruption or destruction would have a serious impact on vital societal functions."*²

In a study conducted in 2008 *"McAfee projected that companies worldwide lost more than \$1 trillion (£708 billion) [...]"*³ within one year due to information security breaches. Often, security breaches were performed by insiders, especially by former employees. Cyber criminals are also increasing their efforts to steal sensitive data and information. The study found that *"criminals will devise increasingly sophisticated schemes to take advantage of employees, new technologies and software vulnerabilities. Attackers will put together increasingly detailed and sophisticated profiles of executives and other targets in order to take spear phishing attacks to the proverbial 'next level'"*⁴

When security breaches can have such dire consequences, both in financial and societal terms, securing the systems is of utmost importance. This applies both for the containment of everyday risks such as failures of individual components and also for preventing malicious attacks from outside against the systems. Figure 1 shows an overview of various types of risks to ICT systems.

To be able to approach such challenges in a professional manner, experts have to collect knowledge on information security, about potential risks and have to create own solutions to reduce them. *"Information Security is usually outlined as the 'preservation of confidentiality, integrity and availability of information' while 'other properties such as authenticity, accountability, non-repudiation and reliability can also be involved'."*⁵

¹ European Network and Information Security Agency. (2009). *Good Practice Guide Network Security Information Exchanges*, p. 8

² Ibid.

³ Knights, M. (2009, January 29). *Security breaches cost \$1 trillion last year*.

⁴ McAfee, Inc. (2009). *Unsecured Economies: Protecting Vital Information*. p. 23

⁵ Glaser, T., & Pallas, F. (2007). *Information Security and Knowledge Management: Solutions Through Analogies?*, p. 2.

Many of these situations occur on a regular basis. For this reason it would be of advantage to allow knowledge sharing between experts, so that the same solutions aren't created over and over again by different individuals. Such a sharing of knowledge could save valuable resources which could be used in more productive ways. Moreover, sharing could lead to solutions of higher quality, due to the fact that existing solutions are enhanced instead of similar solutions being developed all the time.

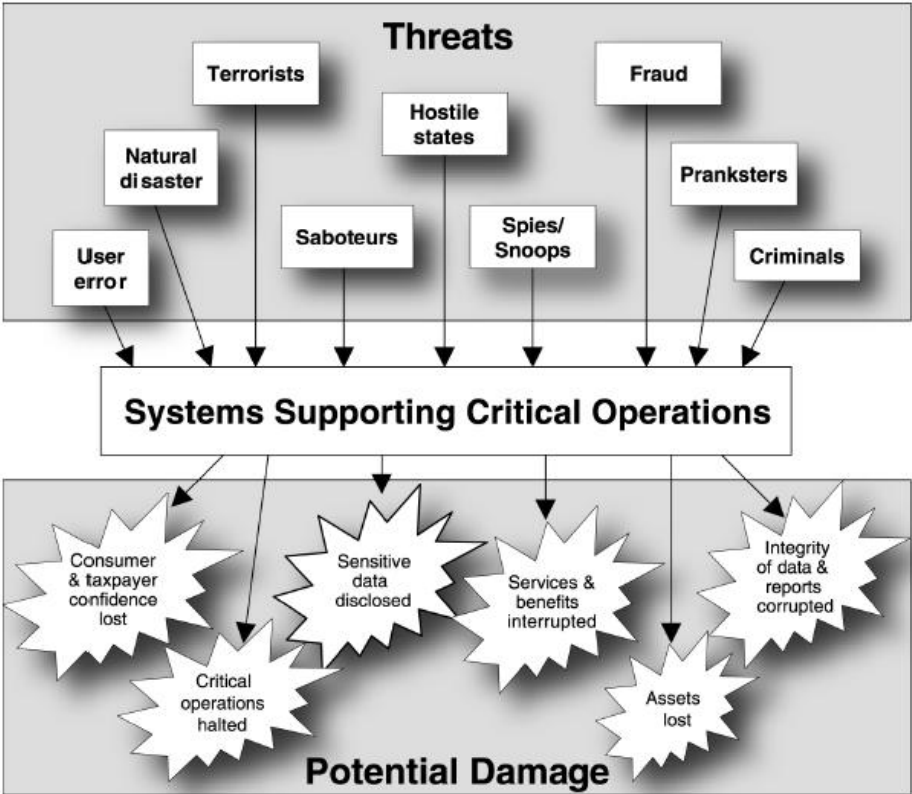


Figure 1: Risks to Computer-Based Operations (US GAO, 2001, p.8)

Till now organizations are partly comparing solutions with other organizations, but there is no unifying system with a widespread basis which could support knowledge sharing in a formal and structured way.

Methods from the field of knowledge management can be useful to create such structured approaches. Knowledge Management has been defined as *"the capability by which communities capture the knowledge that is critical to their success, constantly improve it, and make it available in the most effective manner to those who need it [...]"*⁶.

"Knowledge Management is dealing 'with the process of creating value from an organization's intangible assets' and is about 'the conceptualization, review,

⁶ Birkenkrahe, M. (2002). *How large multi-nationals manage their knowledge*, p. 5

consolidation and action phases of creating, securing, combining, coordination and retrieving knowledge' ⁷.

1.1 Importance of knowledge

Knowledge is a valuable resource to almost every organization. Glaser and Pallas (2007) described the importance of knowledge aptly:

"In our current world of postindustrial value generation, knowledge has become one of the most significant production resources. The existence and success of a growing number of organizations strongly depends on their capability of exclusively using their knowledge for profit generation." ⁸

Knowledge on information security is an important factor to secure the profit generation. Many security incidents occur due to lack of knowledge about security risks, so an effective information security knowledge management could help to reduce certain dangers.

"After decades of mainly technical approaches to Information Security, it is now widely accepted that people are the cornerstone of [information] security" ⁹.

Still, many organizations currently put an effort to solve security risks through technical solutions available on the market while ignoring the fact that security is not just a matter of technical solutions, but also includes people, processes, policies etc. In a rapidly changing environment, systems become more complex and new vulnerabilities are created. *"Technical controls are no longer, in isolation, enough to protect organisations. A combination of people, technology and process is now required."* ¹⁰

In the past, mostly professionals who were aware of security risks were working with information and communication technologies. Nowadays technology has spread so far and is being adopted by most businesses that the gap in knowledge of and skills in technology and especially security is growing. This affects not only individuals, but also organizations as a whole. *"Even professionals who design, build, and supply technology do not always understand the security implications of their decisions."* ¹¹

⁷ Glaser, T., & Pallas, F. (2007). *Information Security and Knowledge Management: Solutions Through Analogies?*, p. 2

⁸ Ibid., p. 1

⁹ Ibid., p. 3

¹⁰ PricewaterhouseCoopers. (2010). *Information Security Breaches Survey 2010 - Technical Report*, p.1

¹¹ Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). *Human Vulnerabilities in Security Systems*, p. 3

PricewaterhouseCoopers (2010) conducted a security survey in UK to assess the state of IT security among organizations. A total of 539 organizations responded to the survey, from small (< 50 staff) to large organizations (> 250 staff). The survey has established some interesting facts that will be presented in the following.

92% of the large respondents had a security incident in the last year, whereas 83% of the small respondents had one in the same period. The average cost of the worst incident a large organization suffered ranged from £280.000 to £690.000. The estimates for overall costs of security incidents in the UK are in the order of several billion pounds a year.

The impact of security incidents can not only be measured in monetary costs. For many organizations an incident has an impact on their reputation as well, which may be even more important than the financial loss. There are also indirect costs that have to be considered, such as investigation and recovery costs.

Direct financial losses can result from loss of assets, but may also include fines imposed by regulators or compensations paid to customers. Direct costs remain relatively small compared to the overall impact of security breaches.

The collected data showed that large organizations have experienced increasing numbers of serious confidentiality breaches. 46% had staff lose or leak confidential data, while 45% of the confidentiality breaches were very or extremely serious.

At the same time the number of organizations with a formal security policy is very high. 90% of the large respondents stated to have a formally documented security policy, 68% have implemented ISO 27001 at least partially. 52% of the large respondents provided staff with ongoing education on security.

A survey among top management operatives of large organizations shows that 77% give a high or very high priority to security. The priority of security for small organizations was even rated higher.

82% of the large respondents and 75% of the small respondents carry out security risk assessment. The most important driver for security is protecting customer information, followed by preventing downtime and outages.

Also there is an increasing trend of convergence of physical and information security management. In the past physical assets needed most of the protection effort, whereas today information assets demand at least an equal level of effort.

This also shows in the investments made in information security. The average expenditure of small respondents was nearly 10 % of the IT budget, for large respondents this value lies at around 6%. Most respondents increased their investments into information security and expect to increase them even further.

Organizations also tend to spend more money on security in response to serious security incidents.

The survey showed that 80% of the large respondents experienced security incidents caused by their staff, either by misuse of systems or unintentional data leaks. Among large respondents, incidents caused by the staff were the most common type of breaches reported. While a large number of the incidents were misuse of the internet and email, nearly half of the large respondents had confidentiality and data protection breaches caused by their staff. Most of these breaches have no malicious intent, but when they occur, their impact are more likely to be serious than other types of security incidents. 45% of confidentiality breaches were very serious or extremely serious.

It could be seen that the extent by which the staff understand the security policy has a big impact on the number of incidents. Organizations in which understanding was poor were twice as likely to have staff-related breaches as those with a good understanding.

In the following section a closer look is taken on the influence of human behavior on information security.

1.2 Influence of human behavior

As was shown in the previous section, behavior of staff members can have a big impact on the security of IT systems. Glaser and Pallas (2007) formulated this as follows: "*To make information security work, people have to behave in a secure manner, must not circumvent established security mechanisms and procedures [...]*."¹²

With the number of security measures increasing due to an increase in security threats, it becomes more and more important to look into the impact these measures have on the individuals. "*The cumulative effect of the demands of several such security mechanisms (e.g. passwords and PINs) at work and at home means that many individuals simply cannot cope and make mistakes.*"¹³

When people have such negative experiences with security measures, they tend to create negative attitudes toward security and lose the motivation to follow security policies. Also when people feel that security mechanisms hinder them in "getting the job done", they try to bypass them. "*High workload, complexity and habitual*

¹² Glaser, T., & Pallas, F. (2007). *Information Security and Knowledge Management: Solutions Through Analogies?*, p. 3

¹³ Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). *Human Vulnerabilities in Security Systems*, p. 3

bypassing of security mechanisms not only increase the likelihood of mistakes, but also create many opportunities for new types of attacks."¹⁴

In order to meet these challenges in information security, some organizations tend to set security policies that are based on security standards, but are handled like *"checklists to satisfy legal or regulatory requirements. Compliance does not lead to effective security if it becomes a box-ticking exercise"*¹⁵, but it leads rather to security measures that are disconnected from the business processes and the individuals they concern.

These policies then have to be enforced through sanctions and increased monitoring and surveillance. These countermeasures can be expensive, threaten the employees' privacy and can lead to a reduction of trust and loyalty towards the company.

Instead, the security policies should be used to communicate that the senior management supports security goals and should also provide an explanation of security decisions to the whole organization. There should be a close cooperation between the management, security practitioners and the employees. Additionally it is important to assess security incidents honestly. To achieve this, *"blame-free incident reporting must be in place: security incidents should be seen as opportunities for learning, where learning takes the form of corrective action review (single-loop learning), and in addition may take the form of preventive action review where the underlying causes of the incident are challenged (double-loop learning).*"¹⁶

Werlinger, Hawkey, & Beznosov (2009) identify several human factors that can lead to security breaches and vulnerabilities: *"lack of security training, lack of a security culture and communication of security issues"*¹⁷.

Security culture in an organization can be built up by increasing the awareness towards security issues, by delivering security education and by security training. Awareness can be raised by attracting the attention of the employees and by making them realise how security issues affect them and others. After people become aware of security topics, they have to be educated in the subject. Education can be delivered through tutorials, courses or other materials. In order to change people's

¹⁴Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). *Human Vulnerabilities in Security Systems*, pp. 3-4

¹⁵ Ibid., p. 5

¹⁶ Ibid., pp. 5-6

¹⁷ Werlinger, R., Hawkey, K., & Beznosov, K. (2009). *Human, Organizational and Technological Challenges of Implementing IT Security in Organizations*. pp. 9-10.

behaviour in security questions, additional training is required. This training should be based in the working context and should address specific security needs.

A lack of security training makes it *"difficult to implement security controls when people do not have enough orientation or education about best IT security practices."*¹⁸ Both lack of security culture and training influence *"the perception of risks that stakeholders have within the organization."*¹⁹

One way to meet security gaps is to identify security issues and to implement policies and procedures to minimize the risks. Here it is important to have effective interaction and communication about security risks between different stakeholders in order to come to a mutual understanding of IT security. Not having a common view of security risks makes it hard to create efficient solutions.

By understanding the security needs of each stakeholder, security solutions can be adapted to the requirements of the users, thus making them more usable and cost effective than *"technical 'one fits all' solutions added onto systems, irrespective of their context of operation"*²⁰.

Understanding the individual needs is also important in order to implement security mechanisms that are integrated into the working processes and that don't interfere with them. When security mechanisms interfere too much and *"create an unreasonable physical or mental workload"*²¹, they are likely to be bypassed.

When designing the security mechanisms, there are a number of principles that can help to create useful solutions. For example, it is essential that security tasks don't significantly reduce the productivity and that they fit into the work process. If a certain security mechanism has to be executed frequently, it should be designed for speed, for infrequently used mechanisms, the design should focus on memorability. Moreover security mechanisms should be designed to minimize the risk of human error and its impact. It is especially important that a single error by an individual should not lead to serious security incidents.

Further, the security culture in an organization should incentivise secure behavior, so that security mechanisms remain effective during the working processes.

Another main challenge concerning information security is the application of knowledge. A lot of the knowledge is available through different media like books, the internet etc., but people seldom use the sources. This can have several reasons,

¹⁸ Werlinger, R., Hawkey, K., & Beznosov, K. (2009). *Human, Organizational and Technological Challenges of Implementing IT Security in Organizations*, p. 10

¹⁹ Ibid.

²⁰ Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). *Human Vulnerabilities in Security Systems*, pp. 6

²¹ Ibid., p. 7

among them insufficient communication between users and information security experts, or a lack of motivation to extract the useful knowledge out of the available sources.

While it may seem to many users that security can be left entirely in the hands of the experts, the consequences of security breaches can be very costly for the entire organization. These consequences may be of financial nature, but can also lead to information leaks, loss of customers, loss of reputation, and compromise of integrity.

The focus of this master thesis is on possible ways of sharing information security knowledge between organizations. Within the scope of this topic the current state of research in the field of information security knowledge sharing will be explored.

This should answer the questions such as how information security knowledge can be shared and what factors influence the willingness to do so.

Moreover, different sharing initiatives and tools are analyzed, in order to explore how these can support information security knowledge sharing.

The second focus of this work is to enhance and to extend the functionality of an existing system for information security knowledge sharing. This system was created to enable information security experts to share their knowledge about information security and security risks of IT systems.

These goals have been brought down to the following research questions (RQ) to verify or to disprove the associated hypotheses.

- RQ1: In which way can knowledge on information security be shared between organizations?
 - Hypothesis 1: Knowledge sharing should ideally take place over a closed joint platform, so that organizations can develop enough trust to expose crucial information. The access to the information over the platform should be regulated to prevent misuse.
- RQ2: How can a tool support knowledge sharing?
 - Hypothesis 2: A tool can provide a central platform for participating organizations over which sharing of knowledge can take place. This allows having more efficient and more structured cooperation than would be possible through classic channels like phone calls or e-mails.

The following chapters will try to answer the research questions. Chapter 2 focuses on two aspects of information security knowledge. In the first part we will discuss how organizations can manage their knowledge and how ontologies and other methods can support them in this task. The second part of the chapter will introduce different

organizational and technological approaches to sharing security knowledge between organizations.

In Chapter 3 an existing web portal for sharing information security knowledge will be presented, followed by a detailed implementation description of several enhancements to the system. Subsequently an outlook is given on further development opportunities.

In Chapter 4 the results of the web portal evaluation are presented. The portal was evaluated by several information security experts, giving constructive criticism and pointing out challenges yet to be addressed.

In the final chapter the findings of this master thesis are summarized, giving an overview of the results and an outlook to future work.

2 Sharing information security knowledge

This chapter focuses on how information security knowledge can be managed within an organization and how this knowledge can be shared with others.

2.1 Managing information security knowledge within organizations

As was shown in the previous section the human factor plays a large role in causing or preventing information security breaches. Often a lack of security training or security culture in an organization is responsible for security breaches that could have been avoided. When information security knowledge is managed effectively within an organization, security issues and policies can be communicated between different stakeholders, so that a mutual understanding is developed. In the following section we will look at the possible interplay between knowledge management and information security.

2.1.1 Knowledge management and information security

*"Knowledge management (KM) provides a formal mechanism for the identification and distribution of knowledge. Benefits of proper KM are improved organizational effectiveness, delivery of customer value and satisfaction, and added product and service innovation."*²²

2.1.1.1 Information Security Knowledge Architecture

In order to apply knowledge management to information security Kesh and Ratnasingam (2007) developed the Information Security Knowledge Architecture (ISKA). This framework can be used to determine the current status of an organization's IT security knowledge and to determine where the knowledge can be improved and what knowledge strategy is required.

As a first step in developing ISKA, the basic concepts were identified using KM concepts. In a second step, interfaces between the components were defined and analyzed.

²² Kesh, S., & Ratnasingam, P. (2007). *A Knowledge Architecture for IT Security*, p. 104

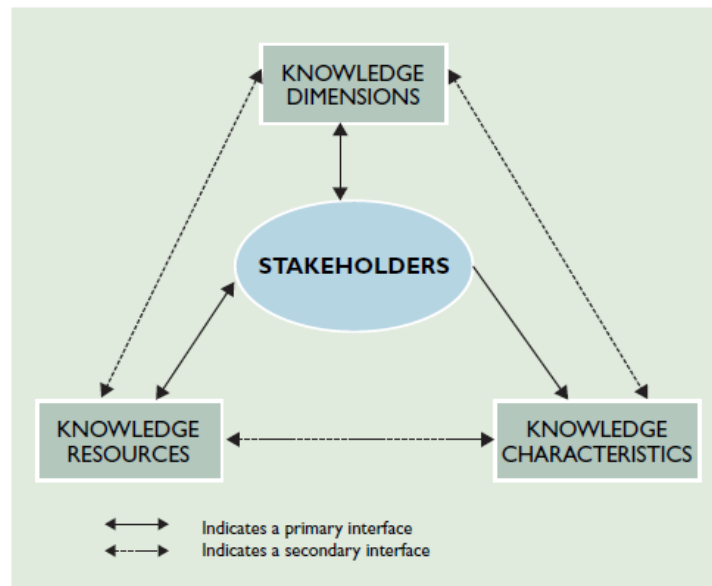


Figure 2: Components and interfaces of ISKA (Kesh, S., & Ratnasingam, P., 2007, p.104).

The identified components were stakeholders, knowledge dimensions, knowledge characteristics, and knowledge resources (see Figure 2). Stakeholders are the people "who should possess IT security knowledge to maintain confidentiality, integrity, and availability."²³ An organization should identify the different roles that IT users have in maintaining information security and based upon this identification, classify their knowledge needs. These roles include Chief Information Officer, Chief Information Security Officer, administrators, etc. A useful scheme for classification is to group the users based on the activities they perform.

The "knowledge dimension" refers to the kind of information the stakeholders should have in order to maintain and to make effective decisions regarding information security. These categories include "Information Security Planning", "Information Security Policy Development", "Security Management Architectures, Models, and Practices", "Risk Management for IT Security" etc.

Information Security Planning "involves both the organizational planning for information security; including tactical, strategic and operational planning, as well as contingency planning."²⁴ Information Security Policy Development includes "enterprise information security program policy, issue-specific security policies, and system-specific security policies."²⁵ The risk management deals with the discovery and the mitigation of IT security risks.

²³ Kesh, S., & Ratnasingam, P. (2007). *A Knowledge Architecture for IT Security*, p. 105

²⁴ Ibid.

²⁵ Ibid.

The "knowledge characteristics" refers to the classification of the available knowledge. Usually knowledge can be classified as either tacit or explicit knowledge. "*Tacit knowledge is unconsciously understood and applied, difficult to articulate, developed from direct experience and action, and is usually shared through highly interactive conversations, story-telling, and shared experience. Explicit knowledge, in contrast, can be precisely formulated and articulated, easily codified, documented, and transferred or shared.*"²⁶ Other classifications include declarative, procedural, social, conditional and relational, pragmatic, and causal.

"Knowledge resources" refers to the knowledge stores that can be either internal or external for an organization. External knowledge can be in form of reports, best practice guides, knowledge networks etc.

Internal knowledge resources can be derived from the "*collective organizational memory*"²⁷ which is based upon past experience and events as documented by members of the organization. "*Such organizational memory systems store the accumulated knowledge, experience, expertise, history, stories, strategies, and successes*"²⁸ of an organization. These systems can be for example "*databases storing the historical data of an organization's significant events and decisions.*"²⁹ Additionally artificial intelligence-based technologies such as neural networks or case-based reasoning can help knowledge management to create new knowledge by merging, classifying and synthesizing existing explicit knowledge. "*Neural network-based systems can analyze patterns of security violations and provide valuable knowledge to stakeholders. Case-based reasoning systems can provide solutions to current security problems by recommending solutions based on similar previous cases.*"³⁰

For an organization it is important to have mechanisms to transform its tacit knowledge to explicit knowledge which then can be stored. Moreover explicit knowledge can also be used by systems as described above.

The ISKA proposes interfaces to connect stakeholders and the other components. These are divided into primary and secondary interfaces.

The primary interfaces represent the relationships between the KM components (knowledge dimensions, knowledge resources and knowledge characteristics) and the stakeholders (see Figure 2).

²⁶ Kesh, S., & Ratnasingam, P. (2007). *A Knowledge Architecture for IT Security* , p. 106

²⁷ Ibid.

²⁸ Ibid.

²⁹ Ibid.

³⁰ Ibid.

The interface between stakeholders and knowledge dimensions maps the knowledge each stakeholder needs and is determined by the security responsibility of each stakeholder. The interface between the stakeholders and knowledge resources refers to the stakeholder's access to the correct IT security information based on the knowledge type that is required. Finally the interface between stakeholders and knowledge characteristics helps an organization to analyze if certain stakeholders have specific characteristics that define their knowledge, for example if a stakeholder holds primarily tacit or explicit knowledge. Analysis of this relationship can help an organization to find appropriate means to convert tacit to explicit knowledge. It can also help to determine if stakeholders have the appropriate knowledge characteristics or if changes are required to better suit information security needs.

The secondary interfaces represent the relationships among the KM components. The interface between knowledge dimensions and knowledge characteristics explores whether certain characteristics such as tacit or explicit are related to the knowledge dimension. The interface between knowledge characteristics and knowledge resources examines if and in what form characteristics are related to certain resources. For example in the case of tacit knowledge, it will be most likely be related to individuals or groups possessing the knowledge. An organization has to identify these holders of information to be able to make use of it.

Finally the interface between knowledge dimensions and resources helps an organization to explore if specific categories of knowledge are linked to certain resources. For example knowledge about setting up certain security measures may come primarily from in-house training.

With the presented "Information Security Knowledge Architecture" organizations can determine the "*quality, completeness, and effectiveness of their IT security knowledge.*"³¹ It can also help to identify and to involve all stakeholders in the security management process, resulting in a more comprehensive coverage of IT security aspects.

2.1.1.2 Adapting techniques from knowledge management

Mittal, Roy and Saxena explain in (Role of Management in Enhancing Information Security, 2010) how tools from the field of knowledge management can help to enhance information security and can be used to effectively use and share knowledge. The authors stated that knowledge management tools can offer means to manage and share information security knowledge within organizations. Before using these tools it is important to put an effort in educating people in information security and raising the awareness for security relevant issues.

³¹ Kesh, S., & Ratnasingam, P. (2007). *A Knowledge Architecture for IT Security*, p. 108

Moreover it is important to decide upon a strategy for knowledge sharing. Knowledge can be codified and be stored in documents, databases etc. or it can be shared informally between people, creating networks and communities.

There are different tools from the knowledge management field that can be used to share knowledge within an organization. These include:

- Content Management: These systems can be used to create content and update information security knowledge like information security standards and best practices
- Knowledge taxonomies: These can be used to easily understand and locate the required information
- Online communities of practice: These can be used for consulting with each other and giving a sense of community to share the knowledge
- Enterprise portals: These can be used as a single point of contact for all the interested stakeholders
- E-Learning: May be used to educate new joiners and to train on the latest developments in the area

Mittal, Roy and Saxena propose in (A Knowledge Management Model to Improve Information Security, 2010) a model using knowledge management techniques to improve information security. This model is composed of three modules that interact with each other:

- Information Security Knowledge Repository: This module stores knowledge related to Information Security
- Information Security Knowledge Sharing and Dissemination: This module includes sharing of information security knowledge, disseminating of knowledge to the concerned stakeholders and updating the Information Security Knowledge Repository with new knowledge created by users.
- Information Security Knowledge Implementation and Effectiveness: This module ensures that information security knowledge is implemented and that the management of such knowledge is effective. The module contains components dealing with incentives for the different user groups such as contributors, users etc.

One important aspect that the authors recommend is the use of incentives to raise the effectiveness of such an Information Security Knowledge Management system. Experts as well as users should get recognition for participating actively in sharing and implementing Information Security Knowledge to increase the overall awareness for security issues. The authors expect that correctly used incentives motivate

stakeholders to use the offered information security knowledge and in the process raise the general security level.

This section showed different approaches of using knowledge management techniques in the field of information security. It was shown that an organization has to be able to determine who the stakeholders are, what kind of knowledge they need and where this knowledge comes from. When these questions are answered, an organization can determine the quality and the completeness of its IT security knowledge, and can explore ways to fill potential gaps, e.g. through content management systems or enterprise portals. The lessons learned in the context of this work are that incentives are required to motivate people to use systems aiming at managing knowledge. Without sufficient acceptance by users the advantages of such systems are minimized.

2.1.2 Capture knowledge in ontologies

There are different approaches of how knowledge can be captured and stored, may they be logical rule sets, databases or ontologies.

In this section we will take a closer look on the use of ontologies. In the context of information security, ontologies can capture knowledge on threats, vulnerabilities, etc., including relations between the different concepts, making this knowledge both human- and machine-readable.

*"Ontologies are agreements about shared conceptualizations. Shared conceptualizations include conceptual frameworks for modeling domain knowledge; content-specific protocols for communication among interoperating agents; and agreements about the representation of particular domain theories. In the knowledge sharing context, ontologies are specified in the form of definitions of representational vocabulary. A very simple case would be a type hierarchy, specifying classes and their subsumption relationships."*³²

An ontology represents a set of concepts (for example entities, attributes, and processes), their definitions and their interrelationships with respect to a given domain.

Vlacheas, Stavroulaki, Demestichas, Cadzow, Ikonomidou, & Gorniak (2011) divided the uses of ontologies into the following categories:

- Communication:

³² Vlacheas, P. T., Stavroulaki, V., Demestichas, P., Cadzow, S., Ikonomidou, D., & Gorniak, S. (2011). *Ontology and Taxonomy of Resilience*. p. 10

Ontologies facilitate shared understanding and communication between people with different needs and viewpoints.

- Interoperability:

Many applications of ontologies address interoperability in which different users need to exchange data either in a practical deployment environment or in development between different software tools. Ontologies can be used in domains such as enterprise modeling and multiagent architectures to support the creation of an integrated environment for different software tools.

- Systems Engineering:

- Specification:

In the specification of software systems, ontologies facilitate the process of identifying the requirements of the system and understanding the relationships among the components of the system. This improved understanding can help distributed teams of designers working in different domains.

Moreover ontologies provide a declarative specification of a software system, which allows to reason about what the system is designed for, rather than how the system supports this functionality.

- Reliability:

Ontologies enable the use of (semi-)automated consistency checking of the software systems with respect to the declarative specification and can be used to make explicit the various assumptions made by different components of a software system, facilitating their integration.

- Reusability:

Ontologies in order to be effective must also support reusability, so that the modules can be imported and exported among different software systems. These ontologies must also be customizable through extension, both to the class of problems and the class of users, allowing the incorporation of new classes of constraints and the specialization of concepts and constraints for a particular problem.

In the following we describe different approaches that use ontologies to represent a variety of aspects of information security.

Mace, Parkin and van Moorsel (2010) suggest capturing information security knowledge in an ontology. This could be an appropriate mean to summarize different sources that influence security policies. By using an ontology approach to capture knowledge, information is formalized as a set of concepts, thus "*creating an agreed-upon vocabulary of IT-security knowledge. The interdependencies between*

fragments of such knowledge will be exposed, facilitating navigation across related information concepts."³³

Schumacher (2003) explains that the development of an security ontology "*enables the automated processing of security-related information*"³⁴ and helps to clarify "inconsistencies" in the used terminology. The developed ontology contains core concepts and relations of the security domain with the primary objective to adopt standard names and definitions of security concepts.

Vorobiev and Bekmamedova (2010) also point to the fact that ontologies can provide the means for "*a common vocabulary to exchange security related information for proper and effective communication*"³⁵. The motivation for this paper was the increasing number of distributed attacks which require a new kind of countermeasures. They argue that collaborative intrusion detection and defenses in distributed environments are needed to face this new kind of security threat. These security measures should have a common mechanism to share the collected knowledge about attacks and possible countermeasures.

This mechanism is based upon several ontologies which reflect different aspects of information security:

- security attack ontology
- security defense ontology
- security algorithm-standard ontology
- security function ontology
- asset-vulnerability ontology

The *Security Attack and Defence Ontologies* can be used as a common vocabulary which store relevant information on attacks and possible countermeasures.

The *Security Algorithm-Standard Ontology* encompasses security algorithms, standards, concepts etc. The *Asset-Vulnerability Ontology* is based on the other security ontologies and is designed as a high level security ontology and is somewhat simplified for non-security professionals.

These ontologies can be used within a single system or within a specified community, where each member can contribute knowledge. As an example the authors describe

³³ Mace, J. C., Parkin, S., & van Moorsel, A. (2010). *A Collaborative Ontology Development Tool for Information Security Managers*, p. 1

³⁴ Schumacher, M. (2003). *Toward a Security Core Ontology*. p. 87

³⁵ Vorobiev, A., & Bekmamedova, N. (2010, February). *An Ontology-Driven Approach Applied to Information Security*. p. 61

an attack, which is detected by defensive components. The attack is added to the security attack ontology as a new class of attacks, while countermeasures are added to the security defense ontology. This approach allows to store and to share developed solutions, so that future attacks can be repelled.

Parkin, van Moorsel, and Coles (2009) develop an information security ontology which aims to further the comprehension of human-behavioral factors as well as to maintain compliance with external standards, which allow organizations to demonstrate that their information is secured.

One goal of the authors is to use the created ontology to inform the decision-making process, *"allowing security managers to account for the identifiable effects [...] that information security mechanisms have upon individuals [...]"*³⁶

This should allow creating solutions that meet not only technical requirements for certain security problems, but also the usability requirements of employees. *"When managing the human element in information security it is necessary to consider both the impact that security mechanisms will have upon the workforce and how they will choose to react to those mechanisms"*³⁷. Taking the human-behavioral perspective into account can lead to a better acceptance of information security measures within the organization.

The developed ontology captures assets, threats and vulnerabilities while including behavioral aspects; for example usability-oriented side effects of certain countermeasures can lead to new vulnerabilities.

Martimiano and Moreira (2006) develop the Computer Security Incident Ontology (ONTOSEC) with a primary focus on computer security incidents. The authors point to the fact, that there are several efforts to classify and store security data without the addition of semantic meaning, which would be important to be able *"to automatically make implicit correlations among security incidents."*³⁸

To achieve this, they propose the application of ontologies which can be used to define a unique vocabulary of concepts and relations related to security incidents.

The concepts in the ontology were adapted from different security incident glossaries and formalized in Protégé using the Web Ontology Language (OWL).

³⁶ Parkin, S. E., van Moorsel, A., & Coles, R. (2009). *An Information Security Ontology Incorporating Human-Behavioural Implications*, p. 46.

³⁷ Ibid., p. 47

³⁸ Martimiano, L. A., & Moreira, E. (2006). *The Evaluation Process of a Computer Security Incident Ontology*. p. 1

The ontology consists of four levels of classes which represent main concepts related to the security incident domain, with a total of 49 classes and 94 properties.

The first level is the core of the ontology and contains some of the main concepts and relations, such as "Agent", "Attack", "Security Incident", "Vulnerability" etc. Figure 3 presents an overview of the first level of the ontology.

Vulnerabilities are defined in a separate Vulnerability Ontology, which is tied into the main ontology. The concepts and relations for the vulnerabilities are based on the Common Vulnerabilities and Exposures Project and the National Vulnerability Database.

After developing their ontology, the authors pointed out, that using ontologies to assist the information security management has several advantages. On the one hand, developing an ontology creates a conceptual model that enhances the understanding of the security incident domain. It can also facilitate the interoperability between different security tools by creating a common way to represent security data and making data and knowledge reusable. As an example for the reusability the Vulnerability Ontology is mentioned, which is imported into the core ontology. In a similar way other ontologies can be tied in and thus extend the knowledge represented in the ontology, for example ontologies focusing on viruses or other forms of computer security threats.

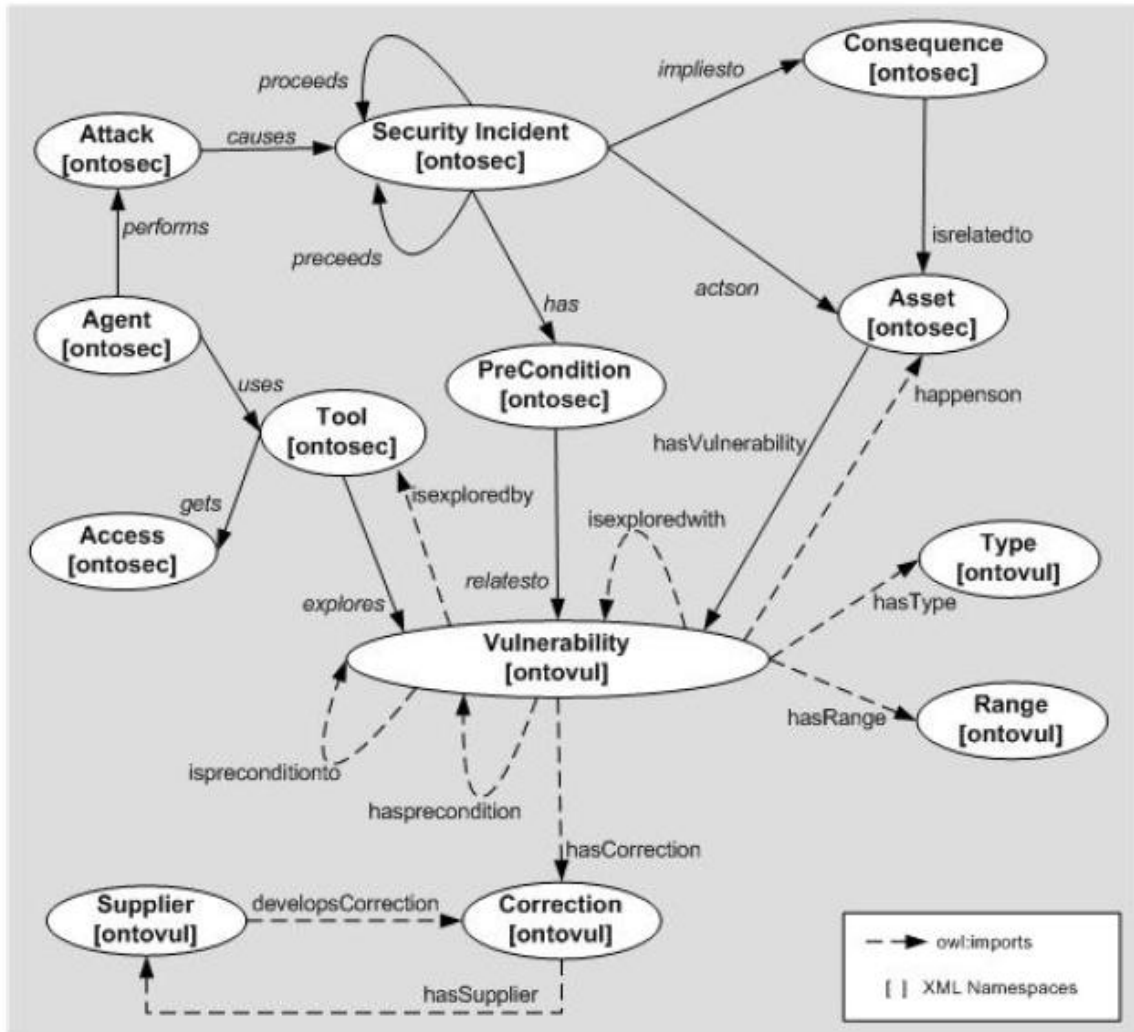


Figure 3: Main concepts of ONTOSEC (Martimiano & Moreira, 2006, p. 5)

Singhal and Wijesekera (2010) develop an ontology with the main goal to capture knowledge about "which threats endanger which assets and which counter measures can reduce the probability of a damage." ³⁹ Additionally, each asset and countermeasure in the ontology is annotated with costs and benefits to enable a quantitative risk analysis. This should help managers of an enterprise in choosing appropriate security mechanisms to reduce threats to their organization.

For the implementation of the ontology the Web Ontology Language and Protégé was chosen, so that the captured knowledge could easily be made portable and shareable.

The concepts shared in the ontology are threats, attacks, vulnerabilities, security mechanisms, assets and risks. Threats are described as a potential for the violation

³⁹ Singhal, A., & Wijesekera, D. (2010). *Ontologies for Modeling Enterprise Level Security Metrics*. p. 1

of security. Attacks are assaults "on a system that violates the security policy of that system"⁴⁰ and exploit vulnerabilities to realize threats.

Vulnerabilities are "characteristics of target assets that make them prone to attack and cause a certain loss or damage."⁴¹ There are standard organizations like the National Institute of Standards and Technology that play an important role in modeling vulnerabilities and maintain vulnerability databases.

Security mechanisms are "designed to prevent the threats from happening or to mitigate their impact when they do."⁴²

Risks are defined as "an expectation of loss expressed as a probability that a particular threat will exploit a certain vulnerability [...]."⁴³

Vlacheas, Stavroulaki, Demestichas, Cadzow, Ikonomou, and Gorniak (2011) use ontologies as a tool to model relationships with the main goal to capture the resilience of IT networks directly and "to encourage the use of ontologies in standards development and in particular for the definition of approaches in standards to provide resilience as a core attribute of a system."⁴⁴ Resilience is defined as a "measure of ability to work through stress and recover to the same initial condition when the stress is removed."⁴⁵

The ontology presented in the paper "offers an open, interoperable and scalable framework [...]"⁴⁶.

Several ontologies were developed to capture the required classes. One ontology represents a model for resilience. The other ontologies examine the business domain, the network domain, the service domain and the domain for information exchange.

Figure 4 shows an overview of the resilience ontology. At the center of the resilience ontology the class "Resilience" is located which is considered as the root for the analysis. It is directly connected with the classes "Threats", "Means", "Domain", "Metrics" and "ThreatAgent".

Threats confront the resilience of a network and can be divided into several subclasses, for example "Security Threats", "Disasters", "Interaction Conflicts" etc. Threats themselves are again divided into subcategories. For example "Security

⁴⁰ Singhal, A., & Wijesekera, D. (2010). *Ontologies for Modeling Enterprise Level Security Metrics*. p. 1

⁴¹ Ibid.

⁴² Ibid., p. 2

⁴³ Ibid.

⁴⁴ Vlacheas, P. T., Stavroulaki, V., Demestichas, P., Cadzow, S., Ikonomou, D., & Gorniak, S. (2011). *Ontology and Taxonomy of Resilience*. p. 43

⁴⁵ Ibid., p. 16

⁴⁶ Ibid., p. 6

Threats" consist of "Interception", "Manipulation", "Repudiation" and "DenialOfService".

A "ThreatAgent" is an entity that threatens "Resilience" and may be human, machine or nature.

"Metrics" are attributes by which "Resilience" can be expressed. These include among others "Availability", "Safety" and "Confidentiality".

The "Means" class represents the means which "have been developed to attain the various metrics and intend to either eliminate threats or fix vulnerabilities."⁴⁷

Means consist of several management functions which include "Fault Management", "Trust Management" or "Supply Chain Integrity Management".

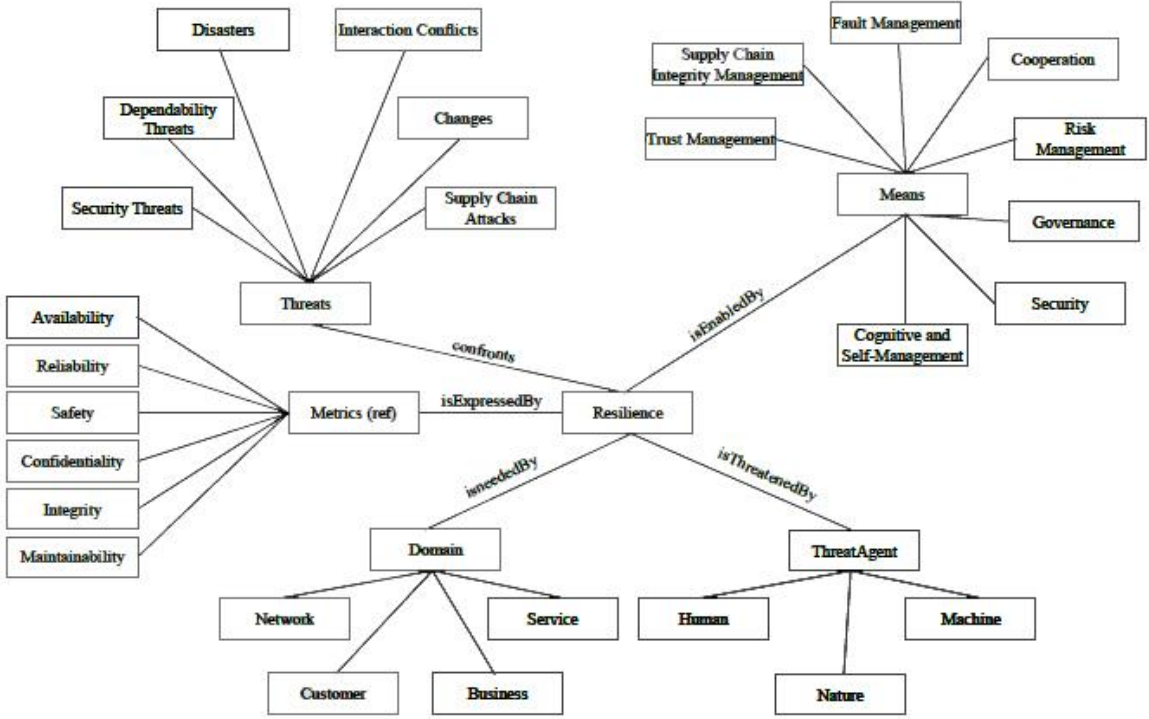


Figure 4: High level overview of resilience ontology (Vlacheas, Stavroulaki, Demestichas, Cadzow, Ikonou, & Gorniak, 2011, p. 25)

Stepanova, Parkin, and van Moorsel (2009) present an ontology that encompasses key elements of the ISO27002 security standard and relates them to each other, so that the impact of security measures can be understood more easily. It also takes human-behavioral aspects into consideration, which can be associated with the captured concepts.

⁴⁷ Vlacheas, P. T., Stavroulaki, V., Demestichas, P., Cadzow, S., Ikonou, D., & Gorniak, S. (2011). *Ontology and Taxonomy of Resilience.*, p. 25

The content of the knowledge base was restricted to guidelines relating to employees' use of removable data storage devices. The ontology was developed using the Ontology Web Language (OWL) and the Protégé Ontology Editor.

The concepts of the ontology are assets, sources and vulnerabilities. In this paper assets are restricted to removable devices and include USB storage devices as well as CDs and DVDs. Sources refer to the standard from which guidelines are taken, in this case ISO 27002 and a toolkit from the University Colleges and Information Systems Association (UCISA).

Vulnerabilities are divided according their nature of being technical (e.g. relating to information security hardware / software infrastructure) or related to human behavior (i.e. part of an activity that requires the interaction with a person).

The authors hope that a separation of technical and human factors can provide a formalized perspective on behavioral issues and their relevance to existing information security management concerns.

Tsoumas, Dritsas and Gritzalis (2005) deal with the "*vague* security knowledge that is present to high-level policy statements."⁴⁸ They present a structured approach to turn informal statements found in these policies and risk assessment documents to "*deployable technical controls*"⁴⁹ that are applicable in the information systems environment. The approach is to create an ontology that elaborates on the security aspects of a system, captures the required concepts and defines a common terminology.

The first step in converting the informal policy statements is to build a security ontology "*in order to simulate the underlying information system.*"⁵⁰

The sources for security knowledge are on the one hand direct sources that are bound to the specific information system, such as organization policies and infrastructure information, on the other hand indirect sources that are implicitly associated with the given information system.

The high-level policy statements offer information about "*the view of organization management on risk avoidance and mitigation issues, ideally aligned with business objectives and goals.*"⁵¹

Indirect sources include security and risk management standards, technical best practices, vulnerability catalogues, etc.

⁴⁸ Tsoumas, B., Dritsas, S., & Gritzalis, D. (2005). *An Ontology-Based Approach to Information Systems Security Management*. p. 155

⁴⁹ Ibid., p. 152

⁵⁰ Ibid., p. 154

⁵¹ Ibid., p. 158

The second step is to gather the security requirements from the policy statements and capture them into appropriate instances of the ontology concepts.

As a next step these requirements should be associated "*with appropriate risk mitigation actions (i.e. specific countermeasures)*"⁵² to create requirement-action pairs. The last step in this approach is to deploy the identified actions to the information system, which can be accomplished for example by "*piping the necessary data to a policy-based management platform.*"⁵³

The security ontology used in the approach is formulated as a Common Information Model (CIM) extension schema enriched with ontological semantics, and is used to model the security management information and the Information Systems security requirements. The ontology was developed by first developing concept-centric partial ontologies, which focused on a central security concept and relations with its direct neighbors, in order "*to be able to approach the Information Systems security concepts from different views and perspectives.*"⁵⁴ These partial ontologies were then integrated into a common security ontology, which was further refined in an iterative process.

As a counterpart to the security ontology a database is created that describes the "*technical actions [...] in order to fulfill the security requirements identified in the security ontology [...], being actually a collection of security controls in a technical level[...]*."⁵⁵ The idea behind this database is to provide solutions on a technical level that address the security requirements of the information system.

At the end of the development process the authors expect a knowledge-based, ontology-centric security management system, that links the high-level policy statements and deployable security controls. The framework as described by the authors may support security experts in the identification of security requirements and the selection of appropriate security controls that meet these requirements.

This section showed an overview of different approaches using ontologies to capture information security knowledge. These approaches support the creation of a common vocabulary of IT security knowledge, which can help clarify inconsistencies and enhances the understanding of the domain. Additionally ontologies are an adequate mean to model relationships between different concepts, helping in modelling the impact that different threats or countermeasures can have. In the context of this work the insights won in this section support the general approach used later in the

⁵² Tsoumas, B., Dritsas, S., & Gritzalis, D. (2005). *An Ontology-Based Approach to Information Systems Security Management.*, p. 152

⁵³ Ibid., p. 154

⁵⁴ Ibid., p. 158

⁵⁵ Ibid., p. 159

information security web portal. By creating a centralized portal accessible to a community of experts, these can collaboratively develop an ontology, creating a common vocabulary and better understanding within this community. By modeling the relationships between different concepts, the captured knowledge can later be used for other purposes, for example for automation within risk analysis and cost calculations.

2.2 Sharing information security knowledge between organizations

In the previous sections different approaches of managing knowledge within an organization were presented. It was shown that tools from the field of knowledge management can be useful in the context of information security and that ontologies can be used to model the domain and to capture knowledge.

While managing information security knowledge within an organization is crucial, the importance to connect and share knowledge is growing. *"It has been recognized that a key factor to improve computer security is the gathering, analysis and sharing of information related to successful, as well as unsuccessful attempts at, computer security breaches."*⁵⁶ This is not only true for individual organizations, but also on a governmental and international level.

Organizations take risks when revealing information about security breaches. This can result in both costs and benefits for the revealing organization.

*"The potential costs of sharing security information can have a snowball effect, accruing from the resultant loss of market share and stock market value from negative publicity. [...] IT executives revealed they were more concerned with the ripple effects of online security breaches on consumer confidence and trust in e-business than the actual financial losses of physical infrastructure. A loss of reputation as a result of reports of information infrastructure violations could be a threat to consumer confidence in a firm's products. Diminished customer confidence and a tarnished reputation, can lead to reduced revenues at an increasing rate."*⁵⁷

However, benefits can also result from mutual sharing of security breach information. For example, future security breaches can be prevented by identifying and fixing vulnerabilities in a combined effort. This then can lead to a better security reputation, which can also have positive economic effects for an organization. It was also shown that *"information sharing by firms can act as a deterrent for hackers, thereby indirectly increasing the effectiveness of security technologies"*⁵⁸

In this chapter sharing of information security between organizations is discussed and some initiatives to advance the topic are presented.

2.2.1 Incentives and barriers

When talking about information sharing, it is important to recognize barriers that can keep stakeholders from contributing their knowledge and to find incentives to overcome these barriers. *"Since knowledge is being regarded as power people are*

⁵⁶ Gal-Or, E., & Ghose, A. (2005). *The Economic Incentives for Sharing Security Information*. p. 186

⁵⁷ Ibid., p. 187

⁵⁸ Ibid.

*motivated to acquire knowledge generated by others but it is unlikely that they share their knowledge altruistically on pure basis of their intrinsic motivation. The result are free riders who use public resources [...] generated by others but do not participate in the creation themselves."*⁵⁹

2.2.1.1 Using incentives to raise effectiveness

In (ENISA, 2010) incentives to information security knowledge sharing were identified and summarized (see Figure 5). The incentives were grouped by their perceived importance.

High	Medium	Low
1. Economic incentives stemming from cost savings; 2. Incentives stemming from the quality, value and use of information shared;	3. The presence of trust among IE participants; 4. Incentives from receiving privileged information from government or security services; 5. Incentives deriving from the processes and structures for sharing; 6. Allowing IE participants' autonomy but ensuring company buy-in;	7. Economic incentives from the provision of subsidies; 8. Economic incentives stemming from gaining voice and influence; 9. Economic incentives stemming from the use of cyber insurance; 10. Incentives stemming from the reputational benefits of participation; 11. Incentives from receiving the benefits of expert analysis, advice, and knowledge; 12. Incentives stemming from participants' personal preferences, values, and attitudes.

Figure 5: Incentives for Information Sharing (ENISA, 2010, p. 13)

The economic incentives are coming from cost savings, which can result "*from quicker reaction to threats, vulnerabilities and attacks, or from anticipating network failures.*"⁶⁰

The second incentive rated as highly important is the quality of the information shared. Part of the motivation to share information is the expectation to receive information of equal value. Additionally the information that is shared must be relevant to participants' concerns to ensure that participants benefit from and maintain participation.

Trust among participants can be found among the medium ranked incentives. For participants it is important to have trust in peers, so that information sharing can take

⁵⁹ Glaser, T., & Pallas, F. (2007). *Information Security and Knowledge Management: Solutions Through Analogies?*, p. 7

⁶⁰ European Network and Information Security Agency. (2010, September). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. pp. 13-14

place. This trust has to be built over time and through personal relationships. It can be based on the perception that other participants have similar desires and intentions. Trust can also be "*backed up by negative consequences (e.g. a legal obligation to share)*."⁶¹

Another medium ranked incentive is the possibility to receive privileged information from government or security services, which is not available from other sources. This information is viewed as high quality information as it also helps finding out "*what government was thinking about a particular issue*."⁶² This incentive is restricted to information sharing networks where governments are involved.

Processes and structures of information sharing can also be seen as incentives to share knowledge within a defined community.

*"To make information sharing real it is essential to lower the practical risks of sharing information through both technical means and policies, and to develop internal systems that are capable of supporting operational requirements without interfering with core business. Consequently, the technical means used must be simple, inexpensive, secure and easily built into business."*⁶³

A clear structure that allows assessing, grading, storing and sharing information can give participants the feeling to be in control of information, which can encourage the sharing of knowledge.

For example "*allowing control of information to rest with the organisation which originally shared it is very important [...]. This means that a participant can share knowing that he is still in control of the information.*"⁶⁴

Agreements among the participants about confidentiality and disclosure can also give an appropriate frame for information sharing. Additionally "*anonymising or particularly anonymising data can ameliorate some of the risk taken by the sharing organisation.*"⁶⁵ On the other hand, anonymizing the information might reduce the weight of the information to recipients. There may be investments of significant resources required to defend against potential violations, so "*the credibility of sources*

⁶¹ European Network and Information Security Agency. (2010, September). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. p. 16

⁶² Ibid., p. 18

⁶³ United States General Accounting Office. (2004). *Critical Infrastructure protection. Establishing Effective Information Sharing with Infrastructure Sectors*. p. 33

⁶⁴ European Network and Information Security Agency. (2010, September). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. p. 19

⁶⁵ Ibid.

is important. *Partial anonymisation, and/or the brokering of information via mutually trusted 3rd parties*⁶⁶ may be considered as useful techniques.

The selected structures should also contain ways to store the information in a secure manner. Suggestions include for example *"effective and secure communications including secure websites"* and the *"provision of an encrypted email and secure web portal to participants"*⁶⁷

Generally it can be said, that it is vital that organizations participating in an information exchange see an economic benefit of information sharing. Cost savings and other benefits are a very good way to incentivize participation and sharing.

*"It is also important that the information shared at an IE [Information Exchange] is relevant to participants, is of high quality (from a reliable trustworthy source), and is at the appropriate level on the operational-strategic spectrum [...]."*⁶⁸

2.2.1.2 Barriers for information sharing

Aside from incentives that encourage participation in an information exchange, there are of course also barriers. In (ENISA, 2010) also potential barriers were summarized (see Figure 6).

High	Medium	Low
1. Poor quality information;	4. Type of participants;	12. Legal barriers related to Freedom of Information;
2. Misaligned economic incentives stemming from reputational risks;	5. Legal Barriers related to fear of legal or regulatory action;	13. Misaligned economic incentives stemming from the costs of participating in IEs;
3. Poor management;	6. Fear or leaks;	14. Misaligned economic incentives stemming from competitive markets;
	7. Group size;	15. Legal barriers related to competition law violations.
	8. Misaligned economic incentives stemming from group behaviour – externalities;	
	9. Social barriers from government;	
	10. Misaligned economic incentives stemming from poor decision-making about investment in security;	
	11. Norms of rivalry;	

Figure 6: Barriers for participation (ENISA, 2010, p. 25)

As the most significant barrier the low quality of shared information was identified. To improve the quality of information, (IAAC, 2002) argues that the submission of pre-analyzed information could mitigate this to a certain degree.

⁶⁶ Messenger, M. (2006, February 13). *Cyber-security: Why would I tell you? Research briefing*. p. 5

⁶⁷ European Network and Information Security Agency. (2010, September). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. p. 19

⁶⁸ Ibid., p. 36

In the short term, this may offer benefits only to other participants in an information sharing community and not to the contributor, but in the long term all participants in such a network could benefit from a higher quality of incident or vulnerability data. The submission of threat, incident and vulnerability data requires the "*assured confidentiality and elaborate safeguards against inadvertent disclosure.*"⁶⁹ Participants may also question if submitting sensitive information is worth the risks of disclosure. The risk of sensitive information being leaked through information sharing can be mitigated through developing trust and ensuring appropriate rules and structures.

Other participants can also be seen as barriers if they are not selected carefully and do not fit into the group. For example there is a strong preference for the participants "*to be technical or security experts, rather than people with responsibilities for sales, marketing or other commercial activities. It was thought that the position of such individuals was incompatible with creating a trusted environment for information sharing, since they would be influenced by commercial considerations.*"⁷⁰

Another barrier can be if participants fear for loss of reputation when they reveal information about an attack or vulnerability risks. Disclosure of such information could also lead to legal action against a participant, thus creating another barrier.

Group size can also be a challenge for information sharing, because if a group is too large, it can be difficult to find common interests and to build up the necessary trust within the group.

A challenge for information exchange can also be an economic misinterpretation of possible benefits from participating. Participants may try to invest less than they contribute in order to benefit from the cooperation. In the most extreme form, this can lead to so-called "free-riders". According to (ENISA, 2010) though, these are not major barriers for information exchange.

An insufficient assessment of the relative benefits and costs as well as an "*aversion to uncertainty could lead to a lack of information sharing because companies do not think it is worth the time or the investment.*"⁷¹

⁶⁹ Information Assurance Advisory Council. (2002). *Sharing is Protecting - A Review of Information Sharing*. p. 22

⁷⁰ European Network and Information Security Agency. (2010, September). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. p. 26

⁷¹ *Ibid.*, p. 31

"Perhaps the greatest barrier to information sharing stems from practical and business considerations in that, although important, the benefits of sharing information are often difficult to discern, while the risks and costs of sharing are direct and foreseeable"⁷²

One barrier that was ranked as of low importance was economic disadvantages from cooperating with competitors. The fear to lose the competitive edge over competitors can hinder the willingness to share information. According to the survey presented in (ENISA, 2010), this is not seen as an important consideration when deciding about exchanging knowledge.

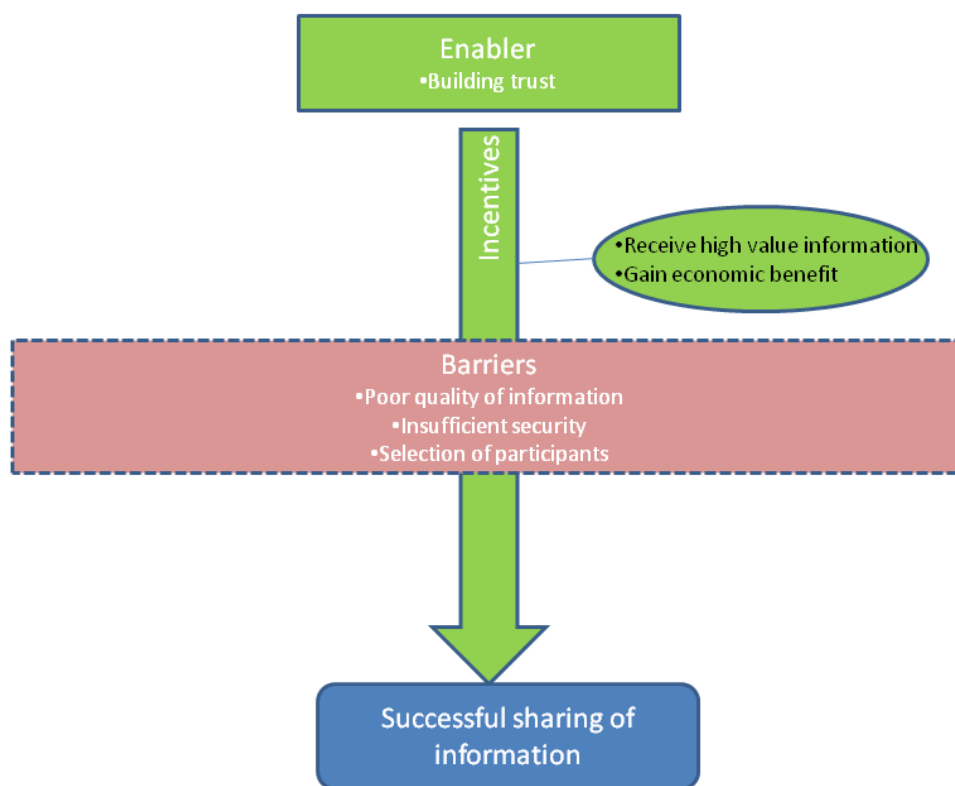


Figure 7: Overview of the most important enablers, incentives and barriers

In this section it was shown that sharing of knowledge is not an altruistic act and has to be incentivized. Studies have shown that the most powerful incentives are economic benefits stemming from sharing knowledge with others. The outlook to receive high value knowledge from others can also serve as a strong incentive. It could also be seen that trust is among the most important factors influencing the willingness to share, while the lack of it is among the strongest barriers. Every effort

⁷² United States General Accounting Office. (2004). *Critical Infrastructure protection. Establishing Effective Information Sharing with Infrastructure Sectors*. p. 33

put into sharing of knowledge has to be aware of this issue and has to put a strong emphasis on building and maintaining trust.

In the context of this work these findings show that a web portal aiming at bringing information security experts together to exchange and share their knowledge has to secure the platform in order to offer a trustful environment. Additionally ways have to be found to attract new members and to incentivize their collaboration.

The next section covers some initiatives dedicated to the sharing of information security knowledge.

2.2.2 Information sharing initiatives

In (IAAC, 2002), different information sharing models were analyzed and presented. It was found that the different approaches can be divided into the following types:

- Educational initiatives: These initiatives aim to raise awareness towards information security issues to improve the preparedness of affected organizations
- Introduction services: The aim of these services is to facilitate the contact between the members of an information sharing community, especially when emergency incident responses are required
- Incident response providers: These provide direct assistance in diagnosing, recovering from and investigating incidents
- Networking services: These aim to facilitate direct networking and information exchange between common sectors through meetings or teleconferences
- Warning initiatives: These aim to collect, process and analyze incident, threat or vulnerability data, and disseminate warnings to a wider audience

These initiatives can be organized in a variety of ways, for example government or military department-managed, government-owned public-private partnership, private sector-owned or in the form of commercial services.

Besides the organizational structures the membership is essential, for it indicates who will receive the shared information. The membership can be aligned vertically along sectoral lines or horizontally along national or regional lines. *"Alternatively, the community may simply be a 'community of interest', in which like-minded organisations may participate as long as they can meet the financial and time costs, do not represent a serious confidentiality risk and bring useful experiences and contacts to the membership."*⁷³

⁷³ Information Assurance Advisory Council. (2002). *Sharing is Protecting - A Review of Information Sharing*. p. 34

The funding models of such initiatives can range from free services over partially free services with additional paid-for options to fully commercial services. "*A median solution - realistically priced services with a range of free and premium service options - offers a sustainable service that balances quality and affordability to a wide range of users.*"⁷⁴

Information sharing initiatives can provide different products that can be divided into five categories:

- Outreach networks: Includes educational products and campaigns, incident response advice etc.
- Meetings: Regular meetings provide occasions for communities to exchange experiences and evaluate trends. Annual and six-monthly meetings are common, but intervals may vary. When well-organized, meetings provide an environment for effective information sharing
- Online discussion forums: Discussion forums are more convenient than physical meetings, but require more attention to anonymity, disclosure and other security issues.
- Aggregated trend, metrics and benchmark products: Data from different participants can be aggregated and analyzed in reports, threat assessments etc.
- Warnings and alerts: "*Warnings provide urgent notification of an impending threat and advise countermeasures and / or increased protective measures. Alerts provide less urgent notification of vulnerabilities and advise on patches and fixes*"⁷⁵

Participating in information sharing initiatives can offer a wide spectrum of advantages. For example sharing initiatives formalize otherwise often informal means of sharing and make them more independent from individual persons. Other advantages include cost- and time-savings.

Over the past decades several information sharing initiatives have been started. In the following, the current effort of the European Network and Information Security Agency will be discussed in detail and additionally some other approaches will be presented in short summaries.

⁷⁴ Information Assurance Advisory Council. (2002). *Sharing is Protecting - A Review of Information Sharing*, p. 35

⁷⁵ Ibid., p. 36

2.2.2.1 Network Security Information Exchange (NSIE)

The European Commission started to assess the "*opportunity of developing the first pan European Information Sharing and Alerting System (EISAS)*."⁷⁶ The European Network and Information Security Agency (ENISA) is responsible for developing this system.

The ENISA regards information sharing as a "*powerful mechanism to better understand a constantly changing environment and learn in a holistic way about serious risks, vulnerabilities and threats, as well as solutions*."⁷⁷ According to ENISA, this is especially true for public e-Communication networks, which form "*an underpinning infrastructure which enables other forms of critical infrastructure such as energy transmission or distribution networks, financial services and transportation*."⁷⁸

In (ENISA, 2009) a concept called Network Security Information Exchange (NSIE) is presented. This exchange is seen as "*a form of strategic partnership among key public and private stakeholders*."⁷⁹ This partnership brings together governments and organizations from the private sector (such as telecommunication companies).

There are already sector-specific information sharing partnerships between the government and the private sector in many European countries. In the UK the Centre for the Protection of National Infrastructure (CPNI) has initiated "*the development of a number of different information sharing models, including sectoral based Information Exchanges [...]*."⁸⁰ Another example is Germany where an Information Exchange is run by the Bundesamt für Sicherheit in der Informationstechnik.

The aim of ENISA is to set up NSIEs in European countries so that on a longer term working relationships can be developed between each country's NSIEs.

The NSIE "*partnership works by exchanging information on cyber attacks, disaster recovery or physical attacks. The drivers for this information exchange are the benefits of members working together on common problems and gaining access to information which is not available from any other source, but only from competitors and national agencies*."

⁷⁶ European Network and Information Security Agency. (2009, June). *Good Practice Guide Network Security Information Exchanges*. p. 6

⁷⁷ Ibid.

⁷⁸ European Network and Information Security Agency. (2010, September). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. p. 5

⁷⁹ European Network and Information Security Agency. (2009, June). *Good Practice Guide Network Security Information Exchanges*. p. 6

⁸⁰ European Network and Information Security Agency. (2010, September). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. p. 8

*Through sharing of experience and sensitive information the groups develops jointly recommendations for mitigating risks and threats and continuously assess existing measures in light of new developments."*⁸¹

In (ENISA, 2009) a number of characteristics of NSIEs are listed to describe how such an exchange network can work. In the following some of these are presented:

- NSIEs address strategic and tactical issues
- NSIEs focus on electronic / physical attacks, malfunctions of systems, interdependencies with other sectors and natural disasters
- NSIEs provide commercial benefits to its members:
There are several benefits from participating in a NSIE, such as cost-savings and improved time to react to serious network failures and *"there are possibilities to influence government policy and avoid the introduction of misplaced regulation."*⁸²
- NSIEs place emphasis on information exchange, not information transfer:
*"NSIEs are peer-to-peer organisations, with flows of information that are balanced in terms of giving and receiving. All members actively share as well as listening."*⁸³
- NSIEs recognize that their members have commercial sensitivities
- NSIEs choose their member carefully to remove barriers to sharing
- NSIEs see Government as having a key role in its creation and operation
- NSIEs are designed to encourage mutual trust:
*"Members are expected to give the same level of information as they receive, under conditions of confidentiality. Keeping membership small fosters trust. The core of the Information Exchange is a set of regular face-to-face meetings."*⁸⁴
- NSIEs members are senior experts with relevant skills:
NSIE members should be experts in the field of information security and resilience with the authority to share sensitive information with their peers and to start changes when needed to address vulnerabilities, risks and threats.
- Meet regularly, face-face, to share sensitive information

⁸¹ European Network and Information Security Agency. (2009, June). *Good Practice Guide Network Security Information Exchanges*. pp. 6-7

⁸² Ibid., p. 15

⁸³ Ibid., p. 16

⁸⁴ Ibid., p. 17

Regular face-to-face meetings are central to the effective working of a NSIE, as they help to establish trust and facilitate the exchange of ideas and information.

- No participation fees for members

Usually the costs of running a NSIE are covered by the government, so that participation fees don't hinder stakeholders in taking part.

- New members require unanimous agreement of existing members

In order to create and maintain trust between members of a NSIE it is important that new members are only accepted on the basis of unanimous agreements.

- NSIEs recognize that incentives are needed for members to participate

*"Most NSIE members see clear benefit in taking part as they receive valuable information from government, and from their sector colleagues. Governments in particular recognise the value of their information as an incentive to encourage others to share information and consequently put significant effort into ensuring its quality and timeliness."*⁸⁵

The listed characteristics show, that one of the key factors of a NSIE being able to operate is mutual trust.

The question of trust must be taken seriously as an information sharing initiative can only succeed if members are able to trust each other. Members take risks when sharing information that might damage their organization in case that it is leaked. Therefore an emphasis has to be put on building trust over time. When the trust is broken, it can be difficult and slow to rebuild. With maturity of trust comes greater value as the higher the trust, the more people feel able to share. One important aspect of trust is that it is personal. Therefore meetings have to take place face-to-face and representatives have to attend. Sending a substitute would not work, since *"a stranger turning up at a meeting would inhibit the sharing of sensitive information. It is important to establish, and consistently use, codes of practice that minimise the risk of breaches of confidentiality, and increase trust. NDA's and different levels of information sharing provide members some protection from unauthorized disclosure."*

⁸⁶

Additional trust building measures are also suggested, for example agreed distribution policies. Adopting widely accepted accredited procedures such as ISO 27000 also helps an organization to become trusted.

⁸⁵ European Network and Information Security Agency. (2009, June). *Good Practice Guide Network Security Information Exchanges*. p. 18

⁸⁶ *Ibid.*, p. 20

After mutual trust is introduced into a NSIE, the next question is what information can be shared. This can reach from single incidents over protocol vulnerabilities to network intrusion information, probing attacks and network configuration issues within standards.

*"To maintain trust NSIEs need to be very sensitive in approaching commercially sensitive issues such as quality of service and availability, which are seen by some private sector members as having significant competitive advantage. Forcing detailed disclosure of such information, for instance, could seriously damage relationships [...]."*⁸⁷

ENISA has observed several types of information that is shared:

- Experiences on threats, attacks, counter measures, responses etc.
- Advisory support in implementing protective measures
- Alert service on attacks and incidents
- Information on cyber security, analysis on threats, risks, impact and vulnerabilities, incidents, security measures etc.
- Information on contingency planning, analysis on threats, risks, impact and vulnerabilities, on single point of failures, dependencies, crisis management arrangements, incidents, exercises, etc.
- Security advisories and best practices
- Any type of information which is deemed interesting and valuable in order to support increasing the NSIE members information security, is collected, disseminated and shared
- Peer good practice
- Incidents and vulnerabilities and also discussions around good practices and recent trends and developments

Information can be shared over web portals with access restricted to members of the NSIE. Usually the website is managed by the government. When trust grows within the group, members also can develop informal links via telephone or email.

ENISA suggests that a variety of information sharing mechanisms should be created to allow more flexibility.

The next sections give short summaries of other information sharing initiatives.

⁸⁷ European Network and Information Security Agency. (2009, June). *Good Practice Guide Network Security Information Exchanges*. p. 27

2.2.2.2 Action 2000

The Action 2000 was a private company established in the UK by the government with the goal to mitigate the threat of the Y2K bug. A core task of Action 2000 was to gather reports of companies about their preparedness for the Millennium bug.

The information collected by the initiative was submitted voluntarily by members who then received a rating for their preparedness. The rating served as a motivation for members to submit reports, since companies who did not enter the reporting appeared as though hiding something.

Information was shared between organizations primarily through meetings, but a Y2K software readiness database and a public website was established as well.

2.2.2.3 Computer Emergency Response Team (CERT)

The CERT, sometimes referred to as Computer Security Incident Response Team (CSIRT), is internally present in many organizations in the sector of government, academia and large industries, and is responsible for incident responses. They often offer helpdesk support and "best practice" trainings.

Usually internal CERTs gather reports from within their organization but also collect and customize external Information Security products and services for the internal audience.

The gathered knowledge is then disseminated through internal systems (telephone, email, intranet).

The model of CERTs can also be expanded to a regional or national level. For example the CERT Co-ordinating Center (CERT-CC) is such an institution. The CERT-CC was founded in 1988 in the USA and offers free service for interested parties. These services include helpdesk support (assist in the detection, interpretation and response to threats), advisories (that highlight vulnerabilities and provide fixes), summaries (that aggregate vulnerability and other data regularly) and practical training and advice on security. The CERT-CC collects information that is voluntarily shared via the helpdesk support, email etc.

The confidentiality of the submitted data is assured through NDAs and submitters also have the option not to share their reports with others.

Information is shared through mailing lists, a website, USENET and other newsgroups.

2.2.2.4 Forum for Incident Response and Security Teams (FIRST)

The FIRST was formed in 1990 after computer security incidents concerning the US Space Physics Analysis Network. Membership to the FIRST is restricted to recognized CERTs or CSIRTs. Information is primarily shared on the Annual Computer Security Incident Handling Conference, where CERT representatives

gather and exchange their knowledge. Additionally mailing lists for members only are used.

The FIRST can recommend and vouch for potential partner CERT teams and therefore encourage trustful relations between its members. Confidentiality is assured by the use of Non-Disclosure Agreements.

2.2.2.5 IT-Information Sharing and Analysis Center (IT-ISAC)

The IT-ISAC started in 2001 as an ISAC specifically for IT-related industry. Members submit their data about security incidents, vulnerabilities and threats voluntarily. The submitted data is filtered and validated.

Confidentiality and legal protection are assured by provider-side anonymization and dissemination only to other members.

The dissemination model includes secure websites, encrypted emails, SMS messaging and telephone in emergencies.

2.2.2.6 National Infrastructure Security Coordination Centre Information Exchanges (NISCC)

The NISCC was founded in 1999 by the UK government as an interdepartmental center for the protection of the Critical National Infrastructure (CNI). Companies relevant in the CNI sector can join the Information Exchanges after agreeing to confidentiality guidelines. Information is exchanged at regular meetings that take place usually every six to eight weeks. The meetings are divided into "closed" and "open" sessions. "Closed" sessions are restricted to full members, while "open" sessions can be attended by other people as well. The "closed" sessions provide a trusted forum for peer consultation where members are trusted to retain confidentiality. This is assured by signing a confidentiality and membership agreement and anonymization of submitted data.

The NISCC collects data from its members, but also from other initiatives like CERTs, Warning Advice and Reporting Points (WARPs) etc.

2.2.2.7 New York Electronic Crimes Task Force (NYECTF)

The NYECTF was formed in 1995 by the US government as a loose confederation of law enforcement officials, public prosecutors, academia and private sector organizations from the banking, finance and ICT sectors. The NYECTF collected data that was submitted voluntarily by its members. The main goal of the initiative was to support member-to-member contact and to develop working relationships between governmental and private sector institutions.

2.2.2.8 Task Force -Computer Security Incident Response Team (TF-CSIRT)

The TF-CSIRT was formed in 2000 by the Trans-European Research and Education Networking Association. Membership is restricted to recognized CERTs or CSIRTs from Europe. Information sharing occurs through regular meetings (four-monthly), the members section of the initiatives website and members-only mailing lists.

The member organizations share their experiences and build trust at the regular conferences, where networking is a primary focus.

Confidentiality is assured by the small size of the TF-CSIRTs trusted circle.

In this section some initiatives were presented that offer organizational solutions to sharing of information security knowledge. Some of these initiatives are specialized on a specific sector; some others aim to bring together stakeholders from different fields. All of these have recognized the importance of trust among the sharing community and have implemented different mechanisms to build and to maintain this trust.

It could be seen that many of the presented initiatives lack concrete technical solutions for sharing knowledge, relying on personal meetings and conventional means of communication.

In the following section some technical approaches for information security knowledge sharing are presented.

2.2.3 Technical implementations of information security knowledge sharing

While the presented sharing initiatives in the previous section discuss the organizational frameworks needed to support the sharing of information security knowledge, there are a few tools that aim at facilitating this task on a technical level. This section presents some tools and frameworks implementing information sharing.

2.2.3.1 Cybersecurity Information Exchange Framework

In (ITU, 2010) a concept for a Cybersecurity Information Exchange Framework is presented. This is intended to offer common means for cybersecurity entities to exchange cybersecurity information. These entities include organizations, persons, objects or processes that possess or seek cybersecurity information, for example CERTs. The presented specifications in the framework are intended to facilitate the exchange of such information and to enhance cybersecurity.

The exchange process as described in (ITU, 2010) consists of the functions depicted in Figure 8.

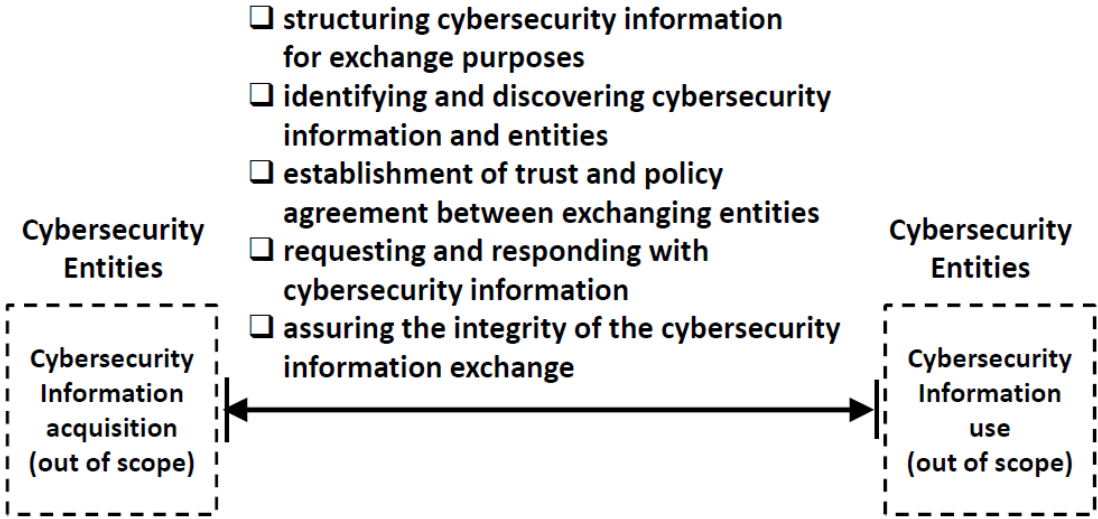


Figure 1: Cybersecurity Information Exchange Process (Rutkowski, 2011)

The framework uses an ontology (see Figure 9) to describe its cybersecurity capabilities. The ontology is "a model for describing the acquisition, accumulation and use of cybersecurity information knowledge that consists of a set of types, properties, and relationships [...]".⁸⁸ Solid lines in Figure 9 indicate a relationship

⁸⁸ International Telecommunication Union - Study Group 17. (2010, December 8). *Draft Recommendation ITU-T X.1500*. p. 10

between information types, while arrows indicate information input from an entity to a knowledge base/database.

This model is used "to define domains for cybersecurity operations, which is then used to identify required cybersecurity entities to support the operations in each domain."⁸⁹

The domains presented are "Incident Handling", "ICT Asset Management" and "Knowledge Accumulation".

The "Incident Handling" domain includes "the detection and response to cybersecurity incidents by monitoring incidents, computer events that constitute the incidents, and attack behavior caused by the incidents. For instance, it detects abnormalities through alarms from detectors, and then builds enumerations by collecting various logs. Sometimes it provides alerts and advisories, e.g. early warnings against candidate threats to user organizations."⁹⁰

The "ICT Asset Management" domain includes operations such as installing, configuring and managing ICT assets within an organization. It also includes operations to prevent incidents as well as operations to control damage caused by such incidents.

The "Knowledge Accumulation" domain generates and accumulates reusable knowledge and includes security-related information.

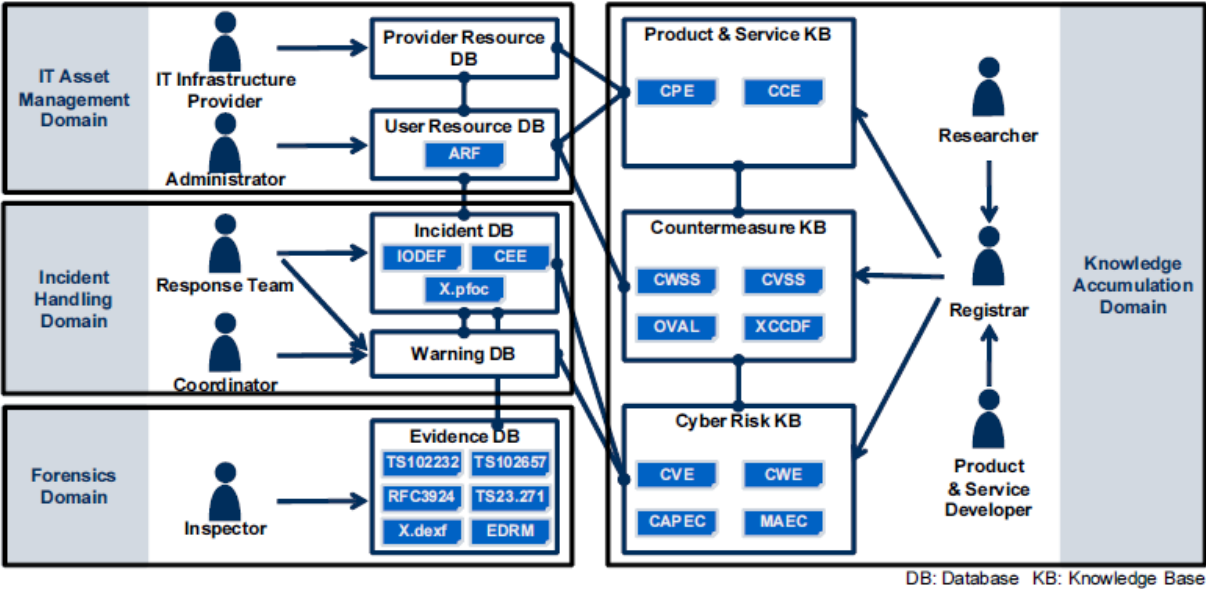


Figure 2: CYBEX ontology model (Rutkowski, Kadobayashi, Furey, Rajnovic, Martin, & Takahashi, 2010, p. 62)

⁸⁹ International Telecommunication Union - Study Group 17. (2010, December 8). *Draft Recommendation ITU-T X.1500*. p. 10

⁹⁰ Ibid., p. 11

There are different entities that are necessary to run the cybersecurity operations described above.

In the "Incident Handling" domain two entities exist. One is the Response Team, which monitors and analyzes the incidents and which may implement countermeasures. The second entity is a Coordinator, who coordinates with other entities and addresses potential threats.

The "ICT Asset Management" domain has also two entities, the Administrator and the ICT Infrastructure Provider. The Administrator is responsible for the system administration and has the information on the ICT assets. The ICT Infrastructure Provider provides each organization with ICT infrastructures, such as network connectivity, cloud computing services etc.

The "Knowledge Accumulation" domain has three entities, the Researcher, the Product & Service Developer and the Registrar. A Researcher researches cybersecurity information and extracts knowledge. The Product & Service Developer possesses information on products and services, e.g. versions, their vulnerabilities, patches and configuration information. The Registrar is responsible for classifying and organizing the knowledge, so that it can be used within an organization.

Each domain has several databases or knowledge bases. The "Incident Handling" domain has a database for incidents containing information provided by the response teams. It also has a warning database with information on cybersecurity warnings provided by response teams and coordinators.

The "ICT Asset Management" domain has a database for user resources, which accumulates information on assets inside an organization, and a database for provider resources, containing information on assets outside of an organization. These include information on resources that an organization uses besides its own assets, such as ICT infrastructure.

The "Knowledge Accumulation" domain contains three knowledge bases: Cyber Risk, Countermeasure and Product & Service.

The Cyber Risk knowledge base contains information on cybersecurity risks and includes knowledge on vulnerabilities and threats. The Countermeasure knowledge base accumulates information on countermeasures to security risks. It also captures *"rules and criteria for assessing the security the security level of ICT assets as well as the checklist of configurations."*⁹¹ Moreover it contains rules and criteria for detecting threats and protecting against them.

The Product & Service knowledge base accumulates information on products and services, which includes knowledge on versions and configurations.

⁹¹ International Telecommunication Union - Study Group 17. (2010, December 8). *Draft Recommendation ITU-T X.1500*. p. 12

To be able to exchange the captured knowledge between entities, it must be structured and described in a consistent manner. (ITU, 2010) defines several "exchange clusters" for distinct cybersecurity user groups and requirements. These are:

- Weakness, vulnerability and state exchange
- Event, incident and heuristics exchange
- Policy exchange
- Evidence exchange
- Identification and discovery
- Identity assurance
- Exchange

*"These capabilities [...] result in an effective cybersecurity ecosystem where knowledge derived from reports, testing, and experience are used to create and evolve the weakness and vulnerability information that in turn can be used together with system state information to 'measure' and enhance security."*⁹²

In (Takahashi, Kadobayashi, & Fujiwara, 2010) this framework is used to discuss cybersecurity in cloud computing.

Cloud computing has several characteristics that set it apart from over environments. One characteristic is the data-asset decoupling. *"Whereas in the non-cloud computing data and assets were tightly coupled, data and assets can be decoupled and manipulated independently in the cloud computing. Therefore, in order to preserve data ownership rights for users, data provenance and data placement change logs are required."*⁹³

Another characteristic is the composition of multiple resources. This requires the capture of three types of information:

"Resource dependency information, security assessment methodologies, and configuration information of multiple resources. Resource dependency information is required to identify who is affected by certain cybersecurity risks and to whom certain cybersecurity information such as warnings and vulnerability needs to be delivered. Security assessment methodologies in cloud computing is, different from those in non-cloud computing, required to be able to assess security levels of multiple resources as one service. Configuration information of multiple resources is required

⁹² International Telecommunication Union - Study Group 17. (2010, December 8). *Draft Recommendation ITU-T X.1500*. p. 14

⁹³ Takahashi, T., Kadobayashi, Y., & Fujiwara, H. (2010). *Ontological Approach toward Cybersecurity in Cloud Computing*. p. 108

to let one service consisting of multiple resources, and let multiple services, work effectively and efficiently."⁹⁴

In the paper changes are suggested to adapt the concept of (ITU, 2010) for cloud computing. For example the incident database has to preserve confidentiality, integrity and availability of an organizations data even if it is in a cloud. It is important that the data is even confidential to the cloud service provider and that manipulation of the data is only possible with appropriate permissions from the data owner.

There are also changes necessary in the warning database. In a non-cloud computing environment users are only warned when they possess or utilize at-risk resources. "*Different from the non-cloud computing environment, a user may utilize a cloud service which may utilize another cloud service that is facing some security risks.*"⁹⁵ Through these dependencies, resources can have indirect security risks and thus users have to be aware of these indirect risks too.

In a cloud computing context, the Cyber Risk knowledge base has to include an impact range of vulnerabilities. This can be accomplished by the use of a resource dependency graph connected to vulnerability information. Besides the impact range, configuration vulnerabilities gain importance in a cloud computing environment. "*Cloud services are based on a combination of multiple components. Therefore, configuration to let the services work takes on a highly important role. Consequently, it is expected that a greater number of vulnerabilities caused by configuration will be found in the cloud computing.*"⁹⁶

2.2.3.2 Web-based tools for collaboration

Donner (2003) argues that there is a need for an ontology to describe security concepts and interrelationships. The internet can be a useful platform for collaboration across the information security community to develop such an ontology. There are numerous web-oriented collaborative tools for the generic creation of ontologies. For example pOWL is a web-based PHP application that offers ontology editing and management and supports the viewing and editing of RDFS/OWL ontologies.

Other tools are for example OntoWiki or Collaborative Ontology Environment (COE). OntoWiki which combines existing Wiki systems with semantic web knowledge representation models where ontologies are represented as "information maps".

⁹⁴ Takahashi, T., Kadobayashi, Y., & Fujiwara, H. (2010). *Ontological Approach toward Cybersecurity in Cloud Computing.*, p. 108

⁹⁵ Ibid., p. 106

⁹⁶ Ibid., p. 107

COE *"builds on the rapid construction techniques of CmapTools and its concept mapping system to represent domain knowledge. An ontology viewing area and collaborative editing environment are combined within COE which then displays ontologies as concept maps. The tool converts these human readable maps into a machine readable ontology language. Concepts from other Web-based ontologies may be incorporated into an ontology, allowing the capture of knowledge from a wide variety of sources."*⁹⁷

One problem with these tools is that they are relatively complex and require extensive training and configuration before knowledge can be captured effectively.

Mace, Parkin, and van Moorsel (2010) describe ontologies as an important step to provide an explicit terminology which allows clear and effective communication among experts and with their clients. It is proposed, that such an ontology should be developed in a collaborative manner.

In this paper the authors discuss their approach to create a web-based tool for collaborative ontology development for the domain of information security knowledge. They advocate collaboration as a mean to create a robust body of knowledge. *"Collaboration must be an integral part of ontology development, allowing multiple experts within the information security domain to capture, integrate, publish and share their knowledge with peers and colleagues. Through collaboration these domain experts can potentially submit, comment on, and peer-review submitted knowledge, with the ultimate aim of reaching consensus."*⁹⁸

The authors identify main features they regard as essential for successful collaborative ontology development. *"These include synchronous/asynchronous communication; proposed content agreement policy; annotation of content and changes; content provenance; concurrency and version control; and personalized views of ontology content."*⁹⁹

In their paper several CISOs were interviewed to understand their view on sharing of security knowledge and on collaboration among experts.

The interviews showed that this collaboration can take many forms, such as formal or informal meetings of experts where discussions and exchange of expertise can lead to joint solutions. This kind of cooperation happens within a known and trusted environment.

⁹⁷ Mace, J. C., Parkin, S., & van Moorsel, A. (2010). *A Collaborative Ontology Development Tool for Information Security Managers*, p. 3

⁹⁸ Ibid., p. 2

⁹⁹ Ibid., p. 3

When trust is limited, experts hesitate to share knowledge that could expose the security situation of their organization. In the paper, the conclusion drawn from this fact is to consider hiding the identity and source of information or to take into consideration the possibility to deal with knowledge at an abstract level as to not betray its source.

As to the acceptance of unknown sources it is important to either have the approval of one or several trusted sources or to be able to test the supplied knowledge in a way with limited negative impact on the organization.

From their interviews with CISOs the authors found several requirements for a collaborative ontology development tool for information security knowledge management:

- Knowledge Capture: The tool must support the capture of formalized knowledge
- Collaboration: The interface should support collaborative capture of knowledge and means to communicate within the user community
- User Guidance: Users should be supported as far as possible through the process of developing an ontology to minimize errors
- User anonymity: Users should be able to *"preserve an appropriate level of anonymity"*. This is important in order to encourage experts to share their knowledge without risking giving away too much relevant information about their organization.

Currently the authors completed a prototype of the tool based on Web-Protégé which supports a number of collaborative features and should help to assess how CISOs could capture and share knowledge.

The tool is composed of a client-side tool interface and the tool server. The interface allows adding, inspecting and manipulating the ontology through a browser-accessible web application. The server part of the tool is stored as a web application archive file on a server. This archive file contains the tool system files as well as the ontology files.

The tool is designed for sharing the captured knowledge and to collaboratively refine the knowledge stored in the ontology. The tool features several means for collaboration such as notes which enable users to annotate, discuss and reach consensus on ontology content.

2.3 Conclusion

In this chapter it was shown that organizations can use knowledge management methods to identify and to collect their existing information security knowledge, determining the quality and completeness of its IT security knowledge. Moreover these methods help to determine who holds which information and where additional knowledge is required. It was also shown that when applying these methods additional efforts are required to motivate people to use knowledge management systems.

It was also shown that ontologies can be used to store knowledge and to create an easily usable representation of the security domain. Different approaches were presented, using ontologies to create common vocabularies of IT security knowledge and to model relationships between different concepts.

Ontologies also have the advantage that they can be integrated into different environments, making them attractive in the context of information sharing. Different approaches were presented, that make use of ontologies to create frameworks for sharing information security knowledge between different organizations.

It could be shown that sharing of knowledge is not an altruistic act and has to be incentivized, most effectively by offering economic benefits and a trustful sharing environment.

Additionally several sharing initiatives that focus on the information security have been presented. All of these have recognized the importance of trust among the sharing community and have implemented different mechanisms to build and to maintain this trust. These initiatives propose organizational solutions for sharing, but often lack specific tools that facilitate the exchange process.

In the following chapter a web tool is presented that aims to support knowledge sharing between security experts. The knowledge is stored in an ontology running in the background, while a web portal offers the necessary user interface to work with the stored knowledge.

3 The security ontology web portal

This chapter describes the security ontology web portal and the development of extensions to support information security knowledge sharing. First, the existing security ontology and the corresponding web portal are presented. Second, the planned changes to the system are discussed, followed by a description of the implementation. Finally further development opportunities are presented.

3.1 The security ontology

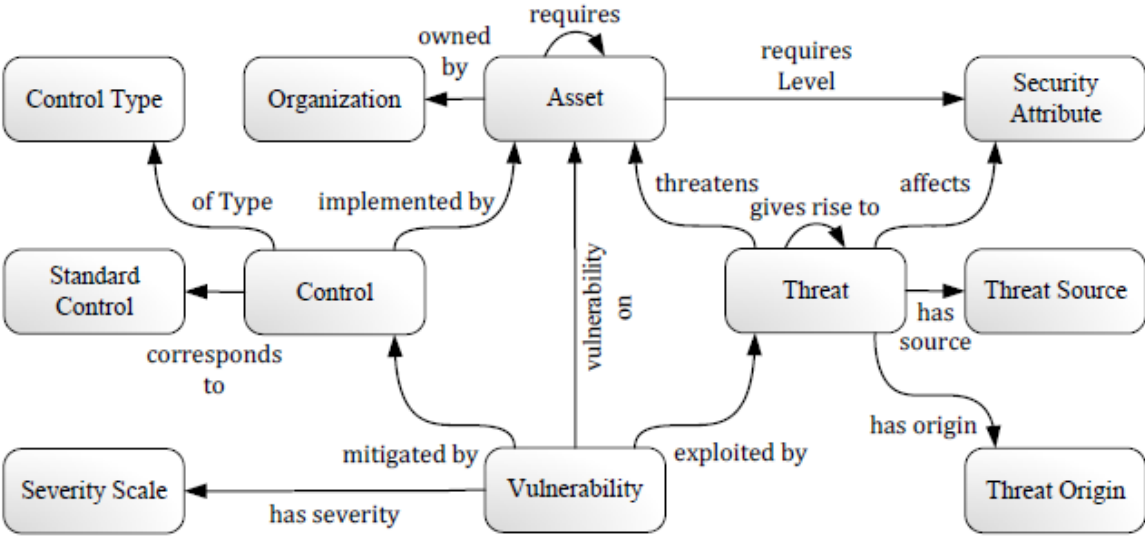


Figure 3: Security ontology (Fenz & Ekelhart, 2009, p. 2)

The presented web portal is aiming to create a unified and machine-readable platform for information security knowledge sharing, enabling collaboration between users, helping them to understand and extend the underlying security ontology together. This approach is not restricted to a certain organization but tries to elevate the collaboration to a global level, crossing organizational and regional borders. Due to the collaborative nature of this approach, a single organization can reduce their costs at knowledge capturing and processing for information security compliance and risk management tasks, since the effort is divided among a larger number of participants.

The security ontology captures different concepts and interrelations within the information security domain. As shown in Figure 10 above, the security ontology consists of several classes, of which the main classes will be described in the following.

The Asset Class

The term "asset" describes all the objects of an organization that generate some business value for the organization. Assets are threatened by threats and are exposed to vulnerabilities, but can also implement controls that mitigate these vulnerabilities.

"The asset concept is categorized either as a tangible or an intangible asset. Typical subconcepts of intangible assets are data, role, software, or reputation. The data concept comprises meta-data on the knowledge of an organization. [...]"

The role concept distinguishes between internal and external roles. Every physical person or organization is connected to one or more roles, which enables a flexible handling if those concepts are to be modeled as control implementations or threatened elements. [...]"

In contrast to the data concept, the software concept has been introduced to provide an ontological structure for those virtual elements which only possess processing characteristics such as text editors, cryptosystems, or operating systems."¹⁰⁰

Tangible assets can be classified as movable (like computers, servers etc.) or immovable elements (like buildings etc.). *"The connections between the asset concepts allow an organization to ontologically map its entire physical infrastructure (including buildings, floors, rooms, computers, alarm systems, etc.)."¹⁰¹*

The Control Class

When implemented correctly, controls can mitigate vulnerabilities and protect the affected assets. Controls can have preventive, corrective, deterrent, recovery or detective measures, depending on the control type.

Controls are derived from and correspond to best-practice and information security standard controls (e.g. ISO 27001)

"Controls are implemented by asset concepts (e.g. fire extinguisher, software firewall, security guard, etc.). Complementary implementations (e.g. the need for smoke detector and a fire extinguishing system) as well as implementation alternatives (e.g. facial scan or fingerprint scan) are incorporated into the knowledge base."¹⁰²

The Threat Class

A threat gives rise to or be a consequence of another threat and potentially endangers an organization's assets. Threats exploit vulnerabilities and are described by potential threat origins (human or natural origin) and threat sources (accidental or

¹⁰⁰ Fenz, S., & Ekelhart, A. (2009). *Formalizing Information Security Knowledge*. p. 4

¹⁰¹ Ibid.

¹⁰² Ibid., p. 5

deliberate source). To model the threat's damage potential, each threat is connected to asset concepts through the "threatens" relation.

The Vulnerability Class

Vulnerabilities are exploited by threats and are in the form of physical, technical or administrative weaknesses. How severe an exploit can be is determined by the severity scale (high, medium, and low). This rating enables a machine to interpret the significance of the vulnerability. Vulnerabilities are bound to assets that take damage when a vulnerability is exploited.

3.1.1 Web portal

In order to enable collaborative, web based editing on the security ontology, a web portal based on Web-Protégé was created. In the following section a short introduction to Web-Protégé and the web portal will be given.

Web-Protégé was developed by the Stanford Center for Biomedical Informatics Research *"as an open source lightweight ontology editor for the web that uses Protégé as its backend."*¹⁰³

The main goal was to develop a web environment that supports a collaborative development of ontologies in a better way. It was designed to provide *"a collaboration platform that is easily customizable for different users and projects' settings."*¹⁰⁴

It offers a browser based web interface for the presentation and editing of ontologies and supports various collaborative features such as commenting and discussing contents.

The browser based nature was chosen to make ontologies more accessible for users without the need to install software. Moreover with the ability to customize the interface it is possible to create useful environments for users who are not ontology experts.

The system is based on a client-server architecture (see Figure 11). On the server side the ontology is accessed through the Ontology API. *"This Java API contains methods for reading and writing OWL ontologies. In addition, the server component provides support for collaboration services, such as annotation of ontology components and change tracking. [...] An important server task is to keep track of the changes in the ontology and to manage conflicts when different clients make changes to the same ontology."*¹⁰⁵

The ontology resides on a Collaborative Protégé server, which provides support for collaboration such as simultaneous editing, transactions and operation atomicity. The task of the Web-Protégé server is to manage the clients.

¹⁰³ Tudorache, T., Vendetti, J., & Noy, N. F. (2008). *Web-Protégé: A Lightweight OWL Ontology Editor for the Web*. p. 2

¹⁰⁴ Ibid.

¹⁰⁵ Ibid., p. 3

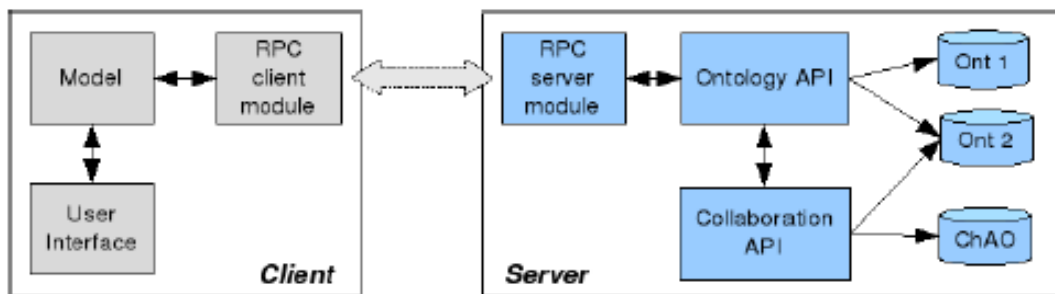


Figure 11: Simplified architecture of Web-Protégé (Tudorache, Vendetti, & Noy, 2008, p. 2)

The server maintains a current version number for each ontology. When a change is made, the ontology's version number is incremented. At a set time interval the clients contact the server to get new changes which are then included in the clients internal model.

"The client side contains the user interface, a model of the ontology on the client and the Remote Procedure Calls (RPC) module to communicate with the server. [...]"

The client has an internal model of the ontology that represents the ontology view of the client. The content of the client model is filled by user interface requests (e.g., get all subclasses of a class), and it also serves as a client-side cache. The user interface components use a listener pattern to register for changes in the client model so that they can refresh when the model changes."¹⁰⁶

Based on this framework a customized version of Web-Protégé was created to enable information security knowledge sharing in the following domains: threats, vulnerabilities, controls, ISO 27001 controls and asset classes. A prototype of the web portal was presented in (Fenz, Parkin & van Moorsel, 2011). Web-Protégé was chosen because it offers an accessible and structured way to share knowledge on a high level among users without the requirement to be experts on ontologies. Moreover it enables registered users to edit, discuss and agree on knowledge, thus supporting the creation of a community that steadily develops the collaborative ontology further for common benefit.

¹⁰⁶ Tudorache, T., Vendetti, J., & Noy, N. F. (2008). *Web-Protégé: A Lightweight OWL Ontology Editor for the Web*. p. 3

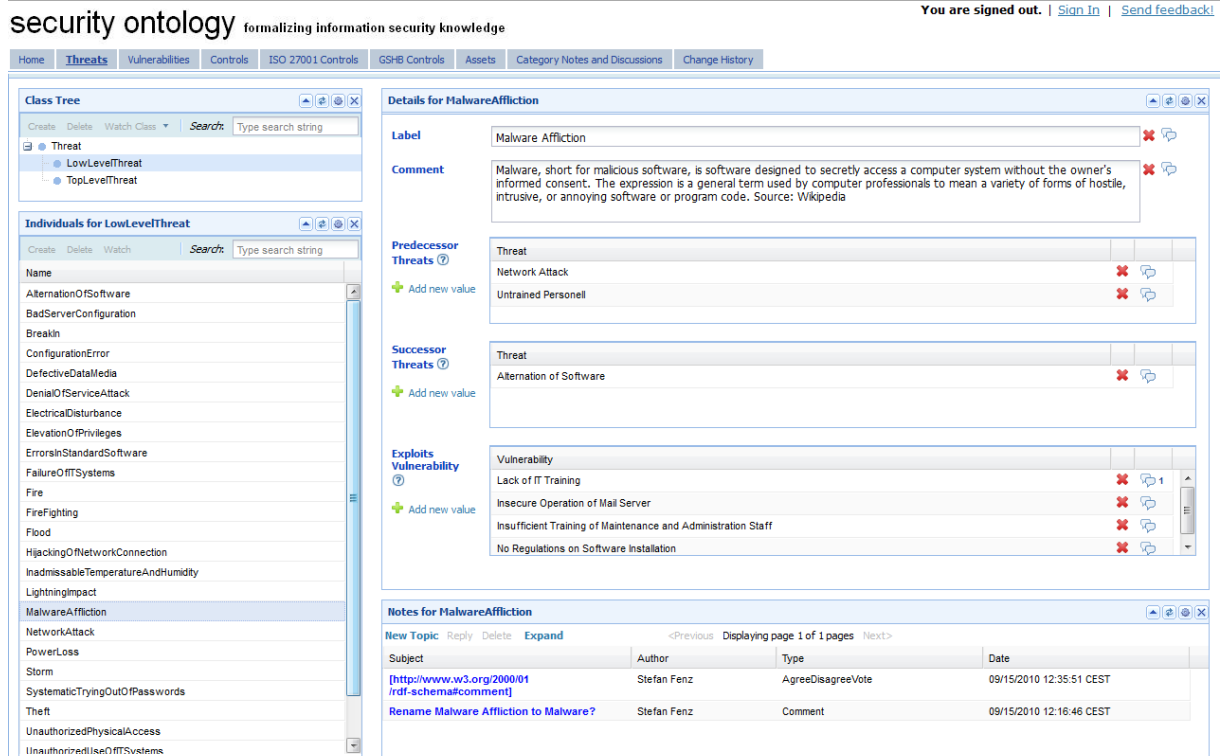


Figure 12 from <http://sec.sba-research.org>

Figure 12 shows the tab for threats in the user interface. The tab contains several portlets such as the class tree portlet for the class "Threat" and a portlet listing the individual threats. Moreover another portlet shows the details of a selected threat. These details are a user defined label, comments, predecessor / successor threats and exploited vulnerabilities.

Web-Protégé supports several collaboration features that allow users to discuss and annotate parts of the knowledge in the ontology. These annotations can also be found in a portlet for attached notes

The home tab is the first tab that is shown to the user after the application is loaded. It contains a short introduction to the platform, a portlet showing the last changes in the ontology and a portlet showing watched entities for logged-in users.

The other tabs are composed of similar portlets like the threats tab, but adjusted for the respective domain (vulnerability, control etc.)

3.2 Extending the security ontology web portal

As the web portal is still under development, there are many areas where functions can be improved and the general functionality can be expanded. Within the scope of this master thesis, required extensions were identified and implemented in the web portal. These extensions range from basic functionality like tertiary entity relations (threats, vulnerabilities etc.) to more complex features like the export of the ontology.

The basic extensions include the option to connect threats, connect vulnerabilities with threats and to use user defined labels to describe entities rather than using internal identifiers. These extensions should improve the usability and general functionality of the web portal.

The incorporation of attributes such as threat source, threat origin, security attribute and control type was selected in order to improve the expressiveness of the ontology and to give users more options to describe threats or controls.

The feedback widget was selected in order to offer the community an opportunity to voice their impressions and opinions, contributing to further development and improvement of the web portal and the security ontology.

The feature to support multiple languages was selected in order to attract users from different countries and regions, enabling them to capture and discuss information security knowledge in their own languages. As seen in (IAAC, 2002), sharing can be organized in different ways, aligned vertically along sectoral lines or horizontally along national or regional lines. Presenting the same content in different languages may support sharing initiatives aligned along national or regional lines, making experts possibly more comfortable at sharing their knowledge.

The export feature was selected to serve as an incentive for participants. As described in (ENISA, 2010), users expect to receive benefits from participating in a knowledge exchange. Therefore, offering them an option to export the collected knowledge from the web portal can be used as an incentive, allowing them to use the ontology within their own system without causing additional costs. Based on the level of participation of users, they can export the ontology as a file that can be imported into a local installation of Protégé, enabling users to customize the ontology to suit their own needs.

The extensions are described in more detail in the following.

3.2.1 Connecting existing threats

In the current version of the web portal, there is no possibility to connect existing individuals. For example, when trying to add a threat as a predecessor / successor, the functionality of the web interface only allows creating new individuals for the class "Threat" instead of creating relations between existing threats.

To give users the possibility to connect existing threats, this option was built in as a widget replacing the current implementation. When selecting an individual threat, users are now able to add predecessor and successor threats from the ontology through the web interface.

3.2.2 Definition of Threat Source, Threat Origin and Security Attribute information for threats and Control Type information for controls

The security ontology specifies additional properties for defined threats and controls, namely "Threat Source", "Threat Origin", "Security Attribute" and "Control Type". The possible values for these properties are not changeable by the portal users, but have to be attached to threats and controls. The "Security Attribute" has to be attached to top level threats, while the "Threat Source" is only attachable to low level threats. "Threat Origin" is applicable to both top and low level threats; the "Control Type" attribute is attachable to all controls.

The web portal did not support these attributes, so an extension of the web interface was implemented in the form of drop-down boxes. The user has now the possibility to choose a value for these attributes, which then are attached to the current entity.

3.2.3 Vulnerability severity definition

The system lacked the possibility to define the severity degree by which a threat exploits a vulnerability. This is an important information for the assessment of the impact of a vulnerability. If a vulnerability is only lightly exploited by a threat, the costs to fix the vulnerability can outweigh the benefits. The other way round, when a vulnerability is heavily exploited, it can be necessary to fix it in order to maintain system security.

Moreover the system did not allow creating relations between existing vulnerabilities and threats. Therefore, an option was created to define relations between existing vulnerabilities and threats in the ontology.

3.2.4 Support of multiple languages

Even though the underlying ontology allows the definition of labels and comments in different languages, the current system did not support different languages, which is a desirable feature due to the collaborative nature of the security ontology.

The implemented modification now allows for setting labels and comments in different languages, selected by the user. These labels are used throughout the web interface where applicable.

This function supports to make the web portal more accessible to an international community and to reduce language barriers. The advantage of this approach is that the knowledge captured in the ontology is not affected, due to the fact that only human-readable labels and comments are changed.

3.2.5 Description of entities by labels instead of internal identifiers

One disadvantage of the initial system was that individuals are presented in the Web-Protégé interface with their internal names as given in the ontology, especially in portlets like the *IndividualsListPortlet* or the *ClassTreePortlet*.

The desired behavior was to show the user human-readable labels instead of internal identifiers, to allow the definition of better suited names for entities in the security ontology, without the necessity to change internal identifiers with the risk to interfere with modeled relations.

Another advantage is that this would enable the use of multiple languages as described in 3.2.4.

3.2.6 Feedback widget

As the web portal is subject to constant development, it is essential to receive feedback from the users. Therefore it is important to offer a simple method to return impressions, opinions and suggestions of users to the system administrators.

In the initial portal version there was only a notice in the top panel of the web portal, asking users to send their feedback to a given email address. Experience showed that this option is often overlooked and therefore not helpful.

As a solution a new feedback function should be implemented through a widget in the home tab of the interface. The placement should be chosen in a way, that users see the widget right away and don't have to look for it.

The widget should be easy to use and offer different options like multiple choice or textual feedback.

When submitted, the feedback should be sent to a predefined email address through the web portal without the need to use an email client on the user's computer.

3.2.7 Ontology export support

Users should have the possibility to download the current state of the ontology to their local systems, so that they can use and adapt it for their own needs. Giving users the opportunity to directly benefit from the web portal should motivate the community to contribute knowledge and enhance the ontology further.

This function was accomplished by offering a download option on the home tab in the user interface.

This option is only available to logged in users to control the distribution of the data. By this, measures can be implemented to prevent "free riders" and to give users incentives to participate in the collaborative development of the ontology. For example a certain level of participation could be defined as a prerequisite to download the ontology to a local computer.

3.3 Implementing the security ontology web portal extensions

As discussed in the previous section, the security ontology web portal is still under construction and offers several opportunities to extend the functionality. In this section the implementation of the previously listed web portal extensions will be explained in detail.

We will begin with the description of the Web-Protégé fundamentals, explaining the implementation of basic elements in the web portal framework, followed by detailed descriptions of the security ontology web portal extensions.

3.3.1 Web-Protégé fundamentals

Web-Protégé is based on the Google Web Toolkit and offers many ways to customize the functionality and the user interface according to the project requirements. In this section basic elements such as configuration and ontology-related issues will be explained and general instructions on how to extend the system will be given.

3.3.1.1 Layout configuration

The Web-Protégé web interface for this project is defined in the XML file called *configuration_Sec.xml*. The default location for the configuration file is in the folder *war/projectConfigurations/*.

*"The layout of Web Protégé is configurable, and it can be easily adapted to different project requirements. The user interface layout is specified declaratively in a XML file. [...] The Web Protégé user interface layout is composed of tabs, e.g. Classes Tab, Individuals Tab, Change History Tab, Notes and Discussions tab, etc. Each tab can contain several portlets that are grouped in a column layout and make up the tab layout."*¹⁰⁷

A tab is split into columns with user defined width. Each tab should have a controlling portlet. The controlling portlet sets the selection for the rest of the portlets in a tab. Whenever the selection in this portlet is changed, that selection is transmitted to the other portlets in the tab to update their display. For example, if a user selects a class in the *Class Tree Portlet* of the *Classes Tab*, this selection affects the other portlets in the tab.

It is possible to add user defined tabs and portlets to the web interface. There are a number of predefined tabs and portlets, but users can also write their own ones. For example, to create a custom tab, users can just add in the XML configuration file an

¹⁰⁷ *WebProtege Layout Configuration*. Retrieved October 16, 2011, from Protégé Wiki: <http://protegewiki.stanford.edu/wiki/WebProtegeLayoutConfig>

edu.stanford.bmir.protege.web.client.ui.tab.UserDefinedTab entry and add any portlet that is needed in it.

For further information on the configuration of the layout, it is advisable to consult the official Web-Protégé wiki¹⁰⁸

3.3.1.2 Web configuration

To configure servlets on the web server and to connect their functionality to specific URLs, it is necessary to adjust the *web.xml* file in the WEB-INF folder of the project. Here, servlets are bound to a URL that can then be called from the client side of the web application. This requires adding the following lines (see Code 1) for each new servlet to the file.

```
<servlet>
    <servlet-name>ExampleServiceImpl</servlet-name>
    <servlet-class>
        edu.stanford.bmir.protege.web.server.ExampleServiceImpl
    </servlet-class>
</servlet>

<servlet-mapping>
    <servlet-name>ExampleServiceImpl</servlet-name>
    <url-pattern>/webprotege/example</url-pattern>
</servlet-mapping>
```

Code 1: web.xml configuration

3.3.1.3 Ontology configuration

The knowledge presented in the Web-Protégé web interface is retrieved from an underlying Protégé server. In Protégé the ontology project is declared as a Database Project working with a database backend. This means that the server itself retrieves the data from a MySQL database containing the ontology. It is possible to convert an OWL file containing the ontology into a database project and vice versa.

The ontology project is connected to a metaproject in Protégé, which administrates defined users, user groups, policies, allowed operations etc.

For further information on how to configure the Protégé server and the database backend, it is advisable to consult the appropriate sections of the official Web-Protégé wiki, especially the guide for administrators¹⁰⁹ and the guide for using a database backend¹¹⁰.

¹⁰⁸ *WebProtege Layout Configuration*. Retrieved October 16, 2011, from Protege Wiki: <http://protegewiki.stanford.edu/wiki/WebProtegeLayoutConfig>

¹⁰⁹ *WebProtege Admin Guide*. Retrieved November 01, 2011, from Protege Wiki: <http://protegewiki.stanford.edu/wiki/WebProtegeAdminGuide>

¹¹⁰ *Working with the Database Backend in OWL*. Retrieved November 01, 2011, from Protege Wiki: http://protegewiki.stanford.edu/wiki/Working_with_the_Database_Backend_in_OWL

3.3.1.4 Portlet definition

To define a new portlet for the web interface, a new class has to be created. This class should be derived from the class *AbstractEntityPortlet*. Once the contents of the class are defined, an entry (see Code 2) in the class *UIFactory* is necessary to be able to use the portlet in the user interface.

```
public static EntityPortlet createPortlet(Project project, String
portletJavaClassName) {

    if (portletJavaClassName.equals(ExamplePortlet.class.getName())) {
        return new ExamplePortlet(project);
    }
    ...
}
```

Code 2: Entry in UIFactory

After the portlet is defined and set in the *UIFactory*, it can be used in the user interface. To add a portlet to the portal, the appropriate entry (see Code 3) has to be added to the project configuration file (see 3.3.1.1).

```
<portlet>
  <name>
    edu.stanford.bmir.protege.web.client.ui.example.ExamplePortlet
  </name>
  <height>100</height>
</portlet>
```

Code 3: Entry in XML configuration file

3.3.1.5 Widget definition

For the extensions of the web portal, new widgets for the *PropertyFormPortlet* had to be defined. In order to create new widgets for the extended functionality of the web portal, classes were derived from existing widgets (e.g. *TextFieldWidget*, *AbstractFieldWidget*, etc.).

After a new widget is created, it has to be specified by an entry in the *FormGenerator* class (see Code 4).

```
protected void createInnerPanelComponents (Panel panel, Map panelConf) {  
  
    ...  
  
    for (String prop : sortedProps) {  
        Object value = panelConf.get(prop);  
        if (value instanceof Map) {  
            String component_type =  
                (String) ((Map) value).get(FormConstants.COMPONENT_TYPE);  
            if (component_type != null) {  
                PropertyWidget widget = null;  
  
                // Entry for new widget  
                if (component_type.equals("ExampleWidget")) {  
                    widget = createExampleWidget(  
                        (Map<String, Object>) value, prop);  
                }  
  
                ...  
            }  
        }  
    }  
}  
  
//Method to create widget object  
protected PropertyWidget createExampleWidget (Map<String, Object> conf,  
String prop) {  
    ExampleWidget widget = new ExampleWidget(project);  
    widget.setup(conf, new PropertyEntityData(prop));  
    return widget;  
}
```

Code 4: Entry in FormGenerator

3.3.1.6 RPC

For some extensions of the web portal, it was necessary to send instructions to the underlying server via RPC. To define a new RPC, three classes have to be created on the client side of the application (see Code 5). The first one is an interface that defines the available methods for the asynchronous call. The second is an interface that extends the interface *RemoteService* and defines a relative path in the web application. The third one is a manager class that is used by classes on the client side to send the RPC to the server.

```
public interface ExampleServiceAsync {

    void processRequest(String example, AsyncCallback<Void> callback);

}

/**
*****
*/

@RemoteServiceRelativePath("example")
public interface ExampleService extends RemoteService {

    public void processRequest(String example);

}

/**
*****
*/

public class ExampleServiceManager {

    private static ExampleServiceAsync proxy;
    static ExampleServiceManager instance;

    public static ExampleServiceManager getInstance(){
        if(instance == null){
            instance = new ExampleServiceManager();
        }
        return instance;
    }

    private ExampleServiceManager(){
        proxy = (ExampleServiceAsync) GWT.create(ExampleService.class);
    }

    public void processRequest(String example,
                               AsyncCallback<Void> callback){
        proxy.processRequest(example, callback);
    }

}
```

Code 5: Classes for RPC

On the server side, a class has to be created that receives the RPC and processes the call. This class has to be derived from *RemoteServiceServlet* (see Code 6).

```

public class ExampleServiceImpl extends RemoteServiceServlet implements
    ExampleService {

    @Override
    public void processRequest(String example)
    {
        ...
    }
}

```

Code 6: Server side implementation of RPC

3.3.1.7 Changes to the security ontology

In order to implement the new functionality, a few changes and additions had to be made to the original security ontology, which will be described in this section.

The extended functionality of the vulnerability widget required a new definition of the relationship between vulnerabilities and threats. To be able to attach a degree to the exploitation relation, the relation between threats and vulnerabilities had to be modeled as a tertiary relationship. A new class called *Exploitation_Degree_Relation* was created which, through the appropriate object properties, connects a threat to a vulnerability and adds a degree in form of the *Exploitation_Degree* class ("None", "Low", "Medium" or "High").

Each individual of the *Exploitation_Degree_Relation* class represents a relation between one threat and one vulnerability with the attached degree, by which the vulnerability is exploited by the threat. This can help to assess if a fix to vulnerability is economically viable.

For multi-language support, the built-in functionality of Protégé was used, which enables the tagging of labels with a language abbreviation (e.g. en, de, fr etc.). To use this, a new class *Language* was added, which represents the available languages in Protégé (e.g. English, German, French etc.). Each individual language has, besides the standard label and comment annotations, an annotation property *hasShortName* which stores the previously mentioned short form of the language. This is necessary in order to be able to match the label language to the language individual.

To store language preferences by users the class *UserProfiles* was added, which stores a profile for each logged-in user and saves the preferred language as soon as this option is selected from the web portal. This allows the web portal to present

certain contents such as label names and comments in different languages as preferred by the user.

3.3.2 Extension 1: Connecting existing threats

One of the major changes made to the existing system is the possibility to connect existing threats. The original system only supported the creation of new entities in order to build a new relation.

To allow the user to select an existing threat from the underlying data store, an edited version of the existing *InstanceGridWidget* was created that disables direct input by the user, but allows opening a selection dialog which offers existing threats. Once the user selects a threat from the list, a connection between the current subject and the selected threat is created. Depending on the property, the selected threat is used as a predecessor or a successor threat. In the following the details will be discussed.

3.3.2.1 New InstanceGridWidget

Based on the original version of the *InstanceGridWidget* a new class named *Custom_Threat_InstanceGridWidget* (see Figure 13) was created, which removed the hyperlink "Add new value" in order to replace it with two hyperlinks, one for each level of threats in the ontology (top or low level). When clicked on, user privileges are checked before the user can alter the knowledge base. In the current version, the user has to be logged in to be able to edit the contents of the web portal. Later a more diverse approach can be taken to specify privileges for each registered user. If the user has signed in to edit the information, a selection dialog is created and opened, that offers individuals from the respective class (Top Level Threat or Low Level Threat). This dialog is discussed in the following section.

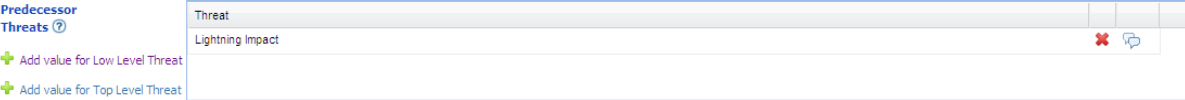


Figure 4: Custom_Threat_InstanceGridWidget

3.3.2.2 SelectionDialog and IndividualsListPortlet

The *SelectionDialog* is created as a new GWT window in the user interface. The *SelectionDialog* (see Figure 14) is defined as an inner class and contains an *IndividualsListPortlet* similar to the ones used to display individuals in the different tabs of the web interface.

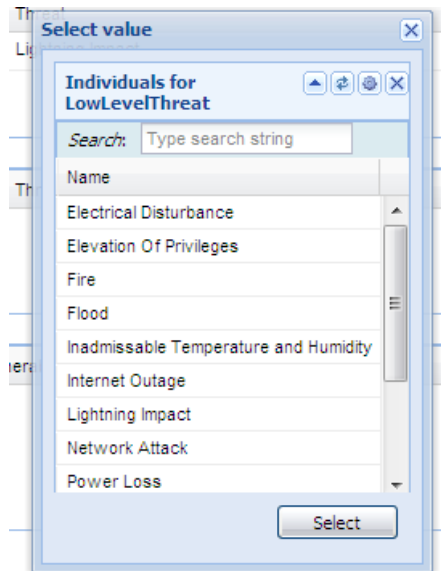


Figure 5: Selection Dialog for individual threats

In order to show only the individuals of a certain ontology class (in this case either Top or Low Level Threat, which is given by *parameter*), the corresponding entity is searched within the ontology through the ontology service manager (Code 7).

```
OntologyServiceManager.getInstance().getEntity(  
    getProject().getProjectName(),  
    OntologyConstants.NAME_PREFIX_ONTOLOGY +  
    parameter.replaceAll("\\W", ""),  
    new CreateSelectableHandler(ilp));
```

Code 7

In the class *CreateSelectableHandler* the returned entity is then set as the main entity of the *IndividualsListPortlet*, so that only individuals of this entity are listed.

During the implementation a conceptual flaw was identified that allowed threats to reference themselves as predecessor or successor. This was corrected by modifying the *IndividualsListPortlet*. When the *IndividualsListPortlet* is created from the *Custom_ThreatInstanceGridWidget* as described above, the current subject is passed on, so that the corresponding element can be removed from the list and therefore confusion is avoided.

Simultaneously a small tweak to enhance the usability was also implemented, which removes the elements from the individuals list that already are in a relation with the current subject. This helps users to keep track of which entities are not yet related to the entity that is currently being edited.

This was implemented by again modifying the *IndividualsListPortlet*. Before the portlet creates the list of possible entities, a list containing the names of entities already in relation with the subject is checked. If an entity is found that is already in a relation, it doesn't show up in the *IndividualsListPortlet*. Therefore users are not being confused by offering them entities in the list that were already used.

When an individual is selected from the list, the selection is registered and forwarded to the method *addRow* (see Code 8).

```
Collection<EntityData> selection =
SelectionDialog.this.selectable.getSelection();
if (selection != null && selection.size() > 0)
{
    EntityData singleSelection = selection.iterator().next();
    SelectionDialog.this.parent.close();
    addRow(singleSelection); // Add selected threat
}
```

Code 8

Here the method *addPropertyValue* in the *OntologyServiceManager* is called, which adds the selected entity as a value of the current property for the edited subject, the response is handled in the class *AddRowHandler* (see Code 9).

```
//Add argument as property value to current property
OntologyServiceManager.getInstance().addPropertyValue(
getProject().getProjectName(),
getSubject().getName(),getProperty(), ed,
GlobalSettings.getGlobalSettings().getUserName(),
getAddValueOperationDescription(), new AddRowHandler());
```

Code 9

After the value has been set, the widget is refreshed so that the new value is recognized by the web interface.

In order to prevent that users edit the individuals while adding connections through the *SelectionDialog*, the *IndividualsListPortlet* was edited so that the toolbar at the top only shows a search field and the option to create a new entity (see Code 10).


```

protected void addToolBarButtons() {
    setTopToolBar(new Toolbar());
    Toolbar toolbar = getTopToolBar();

    ToolbarButton createButton = new ToolbarButton("Create");
    createButton.setCls("toolbar-button");
    createButton.addListener(new ButtonListenerAdapter() {
        @Override
        public void onClick(Button button, EventObject e) {
            onCreateIndividual();
        }
    });

    createButton.setDisabled(!project.hasWritePermission(
        GlobalSettings.getGlobalSettings().getUserName()));
    toolbar.addButton(createButton);

    Component searchField = createSearchField();
    if (searchField != null) {
        toolbar.addText("&nbsp;<i>Search</i>:&nbsp;&nbsp;&nbsp;");
        toolbar.addElement(searchField.getElement());
    }
}

```

Code 10

This customized version of the *InstanceGridWidget* class is then set in the project configuration *configuration_sec.xml* as widget for the *Threat* tab.

3.3.3 Extension 2: Definition of Threat Source, Threat Origin and Security Attribute information for threats and Control Type information for controls

In order to set additional properties for top and low level threats and for controls, drop down widgets were implemented for the properties "Security Attribute", "Threat Origin", "Threat Source" and "Control Type". These were implemented similarly to the *Language_Combobox* in the class *Threat_Misc_ComboboxWidget*. The widget is added in the project configuration, where the widget and the corresponding entities in the ontology are connected.

The widget is generic for all four attributes and first checks the class of the current subject being edited and determines which attribute has to be editable. If an attribute is enabled for editing, the combo box widget is rendered in the property form in the web interface.

When a user changes the value of an attribute, the change is forwarded to the Ontology through the *OntologyServiceManager* (Code 11).

```
protected void onChangeValue(EntityData subj, Object oldVal, Object
newVal) {
    if (!UIUtil.confirmOperationAllowed(getProject())) {
        displayValues();
        return;
    }
    PropertyEntityData pev = new PropertyEntityData();

    if(parameter.equals(OntologyConstants.THREAT_SOURCE)) {
        pev.setName(OntologyConstants.THREAT_HAS_THREAT_SOURCE);
    } else if(parameter.equals(OntologyConstants.SECURITY_ATTRIBUTE)) {
        pev.setName(
OntologyConstants.TOPLEVELTHREAT_AFFECTS_SECURITYATTRIBUTE);
    } else if(parameter.equals(OntologyConstants.THREAT_ORIGIN)) {
        pev.setName(OntologyConstants.LOWLEVELTHREAT_HAS_THREATORIGIN);
    } else if(parameter.equals(OntologyConstants.CONTROL_TYPE)) {
        pev.setName(OntologyConstants.CONTROL_OF_CONTROLTYPE);
    }

    List values = new ArrayList<EntityData>();
    EntityData ed = convertToEntityData(newVal);
    values.add(ed);

    OntologyServiceManager.getInstance().setPropertyValues(
        getProject().getProjectName(),
        getSubject().getName(), pev, values,
        GlobalSettings.getGlobalSettings().getUserName(),
        "Setting miscellaneous attributes",
        new AsyncCallback<Void>() {...});
}
```

Code 11: Change value of threat attributes

3.3.4 Extension 3: Vulnerability severity definition

The widget connecting vulnerabilities and threats is similar to the widget connecting threats with other threats (see Figure 15). It uses the same method to select existing entities through a *SelectionDialog* and the *IndividualsListPortlet*.

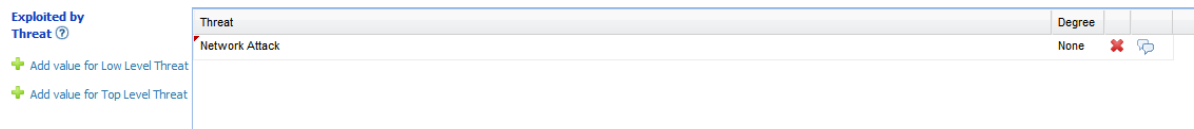


Figure 6: Vulnerabilities Widget

The most important difference between the two widgets is that the relationship between threats and vulnerabilities is modeled as a tertiary relationship between the two and additionally a degree that describes how strong the two are connected.

In the original ontology, the relationship between threats and vulnerabilities was represented by a simple property relation only connecting one with the other directly. In order to be able to give the relationship a weight, it was necessary to model a tertiary relationship as described above.

When a new threat / vulnerability is selected through the *SelectionDialog*, a new individual of the *Exploitation_Degree_Relation* is created in the ontology (see Code 12). This relation entity represents the tertiary relationship. The current subject is set as one end of the *Exploitation_Degree_Relation*.

```
//Create new exploitation relation and set current subject as property value
OntologyServiceManager.getInstance().createInstanceValue(
    getProject().getProjectName(), null, type,
    getSubject().getName(), getProperty().getName(),
    GlobalSettings.getGlobalSettings().getUserName(),
    getAddValueOperationDescription(),
    new AddRowHandler(target));
```

Code 12

When the new individual was successfully created, the remaining property value has to be set, so that the relation completely represents the connection between threat and vulnerability. In the *AddRowHandler* a helper class is called (see Code 13), which sets the selected threat / vulnerability as the target value in the exploitation relation.

When the selected value is set, the exploitation relation represents the connection between the threat and the vulnerability.

```
//Result is the created exploitation relation, target the individual to be
connected to the subject
Exploit_Degree_Helper dgh =
    new Exploit_Degree_Helper(result, target, callingClass);
```

Code 13

After this step is completed, the user can define the strength of the relation between the two entities by selecting an exploitation degree value.

By double clicking on the degree field in the widget, a new *SelectionDialog* opens, which offers different degrees of the class *Exploitation_Degree*, currently "High", "Medium", "Low" and "None" are available.

The selected degree is then set as value for the property "VULNERABILITY_EXPLOITED_BY_THREAT_HAS_DEGREE" through the *OntologyServiceManager* (Code 14).

```
OntologyServiceManager.getInstance().setPropertyValues(
    getProject().getProjectName(), exploit_rel.getName(), pev, values,
    GlobalSettings.getGlobalSettings().getUserName(),
    setDegreeOperationDescription(), new AsyncCallback<Void>() {...});
```

Code 14

3.3.5 Extension 4: Support for multiple languages

3.3.5.1 Select languages

Support for multiple languages is a key feature to enhance the usability for an international user group. While English is defined as the default language, an option has been implemented to define labels and comments in several other languages like German, French, Italian, etc.

For the purpose of managing languages in the web portal, the class *LanguageHelper* was written, which is initialized when the web interface is loaded. It stores the available languages from the ontology (see Code 15), where they are stored as individuals of the class *Language*.

```
OntologyServiceManager.getInstance().getIndividuals(  
    project.getProjectName(), OntologyConstants.LANGUAGE,  
    new FetchLanguagesHandler());
```

Code 15

When widgets are loaded for the web interface, they register themselves with the *LanguageHelper* class. This is necessary so that the widgets can be refreshed when the language is changed. When the current language is changed (by user preference), these widgets are reloaded with labels and comments in the respective language which is defined by the language attribute of these properties in the ontology.

The user preference is set in the Options menu for the logged-in user. Each user has his preference for languages stored directly in the ontology. When the user signs in, his preference is loaded.

If the user hasn't set his preferred language yet, this can be done under the "Edit Profile" option. For this purpose a new class *Language_Combobox* was created. This *ComboBox* shows the languages from the ontology that were loaded in the *LanguageHelper* class (see Code 16).

```

FieldDef[] fieldDef = new FieldDef[]{
    new StringFieldDef("entityData"),
    new StringFieldDef("browserText")
};

RecordDef recordDef = new RecordDef(fieldDef);
Record rec;
languageEntitiesList = languageHelper.getLanguageEntitiesList();

for(EntityData ed : languageEntitiesList){
    Object[] obj = new Object[2];
    obj[0] = ed;
    obj[1] = ed.getBrowserText();
    rec = recordDef.createRecord(obj);
    this.getStore().add(rec);
}

```

Code 16: Language_Combobox is filled with values from LanguageHelper

When a user selects a language he wants to set as his preferred one, his user profile from the ontology is retrieved via the *OntologyServiceManager* (Code 17). If the user has not set the language till this point, a new user profile is created for language settings, and then the language is set. If he already has a profile, only the language is set.

```

OntologyServiceManager.getInstance().getIndividuals(
    project.getProjectName(),
    OntologyConstants.USER_PROFILE,
    new GetEntityHandler());

```

Code 17

3.3.5.2 Description of entities by labels instead of internal identifiers

In order to make use of the defined languages in the application, it is essential to use labels instead of the internal names of the ontology. There are several different widgets, such as the *IndividualsListPortlet*, the *ClassTreePortlet* or the widgets described above, that were modified to make use of labels.

The *ClassTreePortlet* offers the method *computeText*, which returns the text for each node in the class tree. This method was modified to retrieve the annotations for the desired node from the ontology (see Code 18).

```

OntologyServiceManager.getInstance().getAnnotationProperties(
    getProject().getProjectName(),
    entityData.getName(),
    new GetLabelTextHandler(node, watchLabel, entityData));

```

Code 18

A class was defined that should handle the response to the RPC. In this class the label is selected according to the user preference for the language (see Code 19).

When an appropriate label was found that matches the language, this label is set as the text for the node.

```
textBefore = ed.getBrowserText().replaceFirst(
OntologyConstants.NAME_PREFIX_ONTOLOGY, "");
node.setText("");
boolean changes = false;
AnnotationData leftOver = null;
for(AnnotationData ad : result){ //Check all annotations
    if(ad.getName().equals("rdfs:label")){ //If annotation is a label
        if(ad.getLang() != null){
            //If label is of selected language
            if(ad.getLang().equals(selectedLanguage)){
                //Set browser text to label value
                node.setText(ad.getValue());
                changes = true;
                break;
            }else{
                node.setText("");
            }
        }else{
            leftOver = ad;
        }
    }
}
if(leftOver != null){
    if(!changes){ // If no language was found in selected language
        // set text to label without language
        node.setText(leftOver.getValue());
    }
}
if(node.getText().equals("")){ //If absolutely no label was found
    //set label to name in ontology without namespace
    node.setText(textBefore);
}

node.setText(node.getText()+watchLabel);
```

Code 19

This process is done for each node in the class tree, retrieving and setting the labels as the node text instead of the internal class names.

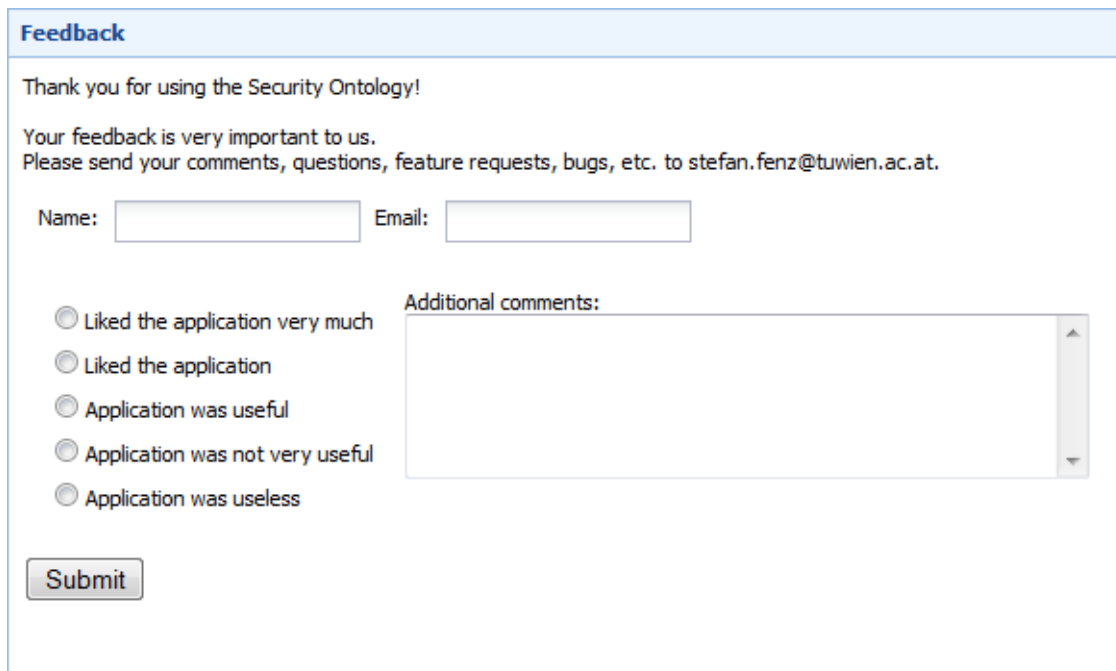
A similar customization was done with the *IndividualsListPortlet*. Here each element of the list is checked for annotations. If an annotation is found in the selected language, it is set as the text for the list element.

Only when no annotation can be found in the ontology, the internal name is used for entities.

3.3.6 Extension 5: Feedback widget

In order to be able to enhance the ontology and the web interface, it is important to receive user feedback. To offer the users the ability to send feedback directly from the web interface, a feedback widget was created and placed in the Home tab. This widget should allow users to directly send their impressions to the site administrator. The decision for the widget to be directly on the first page was made to encourage users to give feedback without having to look for the option. An alternative in the top-side menu of the web interface was explored, but has proven to be easily overlooked.

The feedback widget consists of a form with multiple options to choose from (currently a range from very good to very bad). Additionally space was included for textual feedback, where users can write free-text and are not restricted to given options (see Figure 16).



The screenshot shows a feedback form titled "Feedback" in a light blue header. Below the header, the text reads: "Thank you for using the Security Ontology! Your feedback is very important to us. Please send your comments, questions, feature requests, bugs, etc. to stefan.fenz@tuwien.ac.at." The form includes two input fields for "Name:" and "Email:". Below these are five radio button options: "Liked the application very much", "Liked the application", "Application was useful", "Application was not very useful", and "Application was useless". To the right of these options is a text area labeled "Additional comments:" with a vertical scrollbar. At the bottom left of the form is a "Submit" button.

Figure 16: Feedback widget

Moreover, users can enter their name and email address, thus enabling administrators to respond to questions and suggestions in the feedback. It may also be useful in the case that specific accounts should show erratic behavior.

When the user decides to submit his feedback, a text is composed which takes the information out of the feedback form (see Code 20). Subsequently the text is sent to an email address which has to be specified together with the other email related properties.


```
String body = "Results:" +
    "\nName: " + nameField.getValueAsString() +
    "\nAddress: " + address +
    "\nChoice: " + choice +
    "\nText: " + textArea.getValue();
```

Code 20

This step is being performed through the class *EmailServiceManager*, which offers the method to send the email (Code 21).

```
//send Email through RPC call
EmailServiceManager.getInstance().sendEmail(
    WebConstants.FEEDBACK_RECIPIENT ,
    "Feedback", body, address,
    new AsyncCallback<Void>(){...});
```

Code 21

For the transmission of the email the built-in class *EmailUtil* is used, which offers the function to send emails, given that the application properties are set correctly, including the SMTP server and account settings, like username and password.

For convenience these properties were saved in the separate class *WebConstants* to allow easy editing of the settings.

3.3.7 Extension 6: Ontology export support

As described in Section 3.2.7, an option to download the current state of the ontology should be provided to registered users.

The option to export the ontology from the Web-Protégé interface to a downloadable OWL file was implemented as a widget in the Home tab (see Figure 17). Logged-in users can click on a link that starts the export process and then offers a file download.

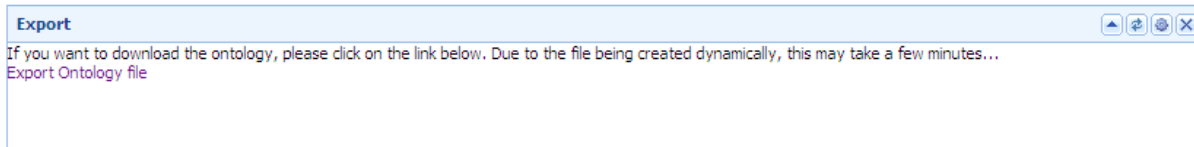


Figure 17: Export widget

If the user is not logged in, a message box pops up that asks the user to login. The login is required in order to have a regulation of who is allowed to download the ontology. By this measure it is possible for example to define a minimum level of participation that is needed before a user can download the knowledge gathered in the ontology, thus giving users an incentive to add their own knowledge to the collaborative security ontology.

When the user clicks on the link offered in the portlet, a HTTP GET-request is sent to the URL specified in the *web.xml* file. The URL points to the servlet class that should process this request; in this case the task is forwarded to the *ExportFileServlet*.

This servlet then generates a response to be sent to the client's browser (see Code 22).

```

ServletOutputStream out = response.getOutputStream();
ServletContext context = getServletConfig().getServletContext();
ExportOntologyServiceImpl export = new ExportOntologyServiceImpl();

File file = export.exportFile(OntologyConstants.PROJECT_NAME); // Create OWL
file to return to client
String mimetype = context.getMimeType(file.getName());

response.setContentType((mimetype != null) ? mimetype : "application/octet-
stream");
response.setContentLength((int) file.length());
response.setHeader(
    "Content-Disposition",
    "attachment; filename=\"" + file.getName() + "\"");

DataInputStream in = new DataInputStream(
    new FileInputStream(file)); //Create DataInputStream from file

int length;
while ((in != null) && ((length = in.read(byteBuffer)) != -1)) {
    out.write(byteBuffer, 0, length);
}

in.close();
out.flush();
out.close(); // Close stream to client

```

Code 22

The servlet calls the export function in the *ExportOntologyServiceImpl* class, which creates the OWL file to be returned to the client.

The actual file export was adapted from the class *JenaExportPlugin* that originally handles exports from Protégé to an OWL file. This method has also proven useful to handle the export from Web-Protégé, which in its current form lacks an option for export of ontology knowledge.

In order to export the knowledge to a file, first the knowledge base of the current project is extracted to an object of type *KnowledgeBase*. Then a path is specified to which the exported file should be saved. In order to have comprehensive names, the files are named with appended date to mark the extraction date.

The extracted knowledge base is then passed on together with the created path to the method *exportProject(...)*, which as described before is based on the Jena plugin. Here the *OWLModel* is extracted from the knowledge base and the writer for the OWL file is configured. In order to write the exported data to a file, the *JenaWriter* was chosen due to unsatisfactory results with the native Protégé writer. Code 23 shows an extract of the actual export process, where the ontology model is extracted and then is written into a file that was specified through a file URI.

```

OntModel newModel = ((OWLDatabaseModel) oldOWLModel).getOntModel();
OWLDatabaseModel dbModel = (OWLDatabaseModel) oldOWLModel;
String xmlBase =
dbModel.getTripleStoreModel().getActiveTripleStore().getOriginalXMLBase();
String defaultNS = dbModel.getNamespaceManager().getDefaultNamespace();
if (xmlBase == null) {
    if (defaultNS != null && defaultNS.endsWith("#")) {
        xmlBase = defaultNS.substring(0, defaultNS.length() -1);
    }
}
try {
    File file = new File(fileURI);
    JenaOWLModel.save(file,
        dbModel.getOntModel(),
        FileUtils.langXML,
        defaultNS , xmlBase);
    return file;
} catch (Throwable t) {
    print("Errors at exporting the OWL Database to OWL file");
    print("Error: "+t.getMessage());
}

```

Code 23 (Adapted from <http://smi-protege.stanford.edu/repos/protege/owl/trunk/src/edu/stanford/smi/protege/owl/jena/export/JenaExportPlugin.java>)

As a result of the export operation the OWL file is created on the server under the given file path. Additionally the result is returned as a File object which then is returned to the *ExportFileServlet*. The servlet sends the file over a data stream (see Code 22) to the client's browser, invoking a "Save as..."-dialog. Through this dialog the user can save the generated file to his local machine, where he can import it into a local distribution of Protégé, thus able to edit and customize the security ontology with own knowledge and data, e.g. about local assets, specialized threats etc while still having the general knowledge collected in the web ontology.

After conducting the evaluation of the web portal, it was found that placing the export function in the panel at the top of the page would be more visible to the users. Therefore the widget was removed and the functionality was moved to the top panel.

4 Evaluation of the security ontology web portal

For the purpose of evaluating the implemented functionality of the security ontology web portal, an evaluation process consisting of multiple phases was conducted.

The goal of this process was on the one hand to review the usability of the web portal functions and on the other hand to assess if the tool can support information security knowledge sharing among information security experts.

For the evaluation we selected three experts with at least five years of information security expertise. All three experts work in Austrian small- and medium-sized enterprises that are specialized in offering information security services and products. The evaluation process is structured in three phases:

Within the first phase we introduced the participants to the security ontology and to the corresponding web portal. This introduction covers (i) the general purpose of the security ontology, (ii) an overview of the captured concepts, (iii) and a general overview of the main functions of the web portal.

Within the second phase we assigned three assignments to the participants (adding new knowledge, editing existing knowledge, and exporting the knowledge). Only a brief introduction to the web portal was given, to evaluate how intuitive the interface is.

Within the third phase we gathered user impressions and opinions about the web portal by structured and open questionnaires.

4.1 Assignments

4.1.1 Assignment 1

The first assignment should help to get familiar with the web portal. As a first step the user should login with a provided test account. Then he should select his preferred language in the user settings. After this is done, the participant should take one threat or vulnerability and add additional knowledge to the existing one by editing the commentaries in his preferred language. Afterwards the participant should get familiar with the function to connect threats and vulnerabilities by adding new relations between existing entities.

4.1.2 Assignment 2

In the second assignment, the user should create new threats and vulnerabilities. As a new low level threat the participant should add "Earthquake" and connect it with the successor threat "Asset Damage". If other appropriate relations between the threat

"Earthquake" and other threats or vulnerabilities are found, these should also be defined in the portal.

As a new vulnerability the user should add "Insufficient training on IT security". As a low level threat exploiting this vulnerability, "Untrained personnel" should be added. An appropriate vulnerability exploitation degree should also be assigned to this relation.

The vulnerability should be connected to controls that can mitigate it. The user should define the control "IT security training" and create a relation between the vulnerability and the control.

The threat "Untrained personnel" should also be connected with predecessor and successor threats were applicable (for example "Data Loss" as a successor threat).

Each new entity should be described with a label and describing commentary in the preferred language selected in the user settings.

4.1.3 Assignment 3

As the final assignment participants should use the export function on the home tab to export the ontology into an OWL file. Afterwards the user should load the OWL file into a local ontology project in Protégé.

4.2 Questionnaire: Impressions and opinions

4.2.1 Questions about assignments

1. How easy or difficult was it to complete the assignments?
2. How long did it take to complete them? Was the time appropriate or do you feel it took too long?
3. Do you think that there is a way to complete the assignments more efficiently? If so, what are your suggestions?

4.2.2 General questions

1. How did you like the layout of the web portal?
2. Was the user interface clear enough to be able to use the tool right away or was an explanation needed?
3. Was the structure of the security ontology clear?
4. Did you have problems with terminologies used in the ontology?
5. Do you find the knowledge captured in the ontology useful?
6. Could you benefit from using such a tool in your every day work?
7. Do you think that the web portal offers you enough functions to express your knowledge on the subject? Or are you missing tools that could enhance the expressiveness?
8. Would you contribute your own knowledge to this or a similar web portal? If not, please explain
9. Do you think that this tool can support the exchange of security knowledge between experts of different organizations? Please explain
10. Would you edit contributions made by other users, e.g. correcting them or adding facts?

4.3 Analysis of collected data

This section contains the results of the evaluation process, which was performed with three information security experts, who will be called IS1, IS2 and IS3.

First the participants are introduced briefly to the security ontology, followed by their general opinions on information sharing and finally their views on the web portal and the performed assignments are presented.

4.3.1 Participants

IS1 is an IT and security specialist with more than 5 years of professional experience in the field. The organization he is working for is a SME with a special focus on secure software development.

IS2 is a security specialist with 5 years experience and is working in the IT security consulting sector.

IS3 works as a security specialist with about 5 years of work experience and is currently working at a small-sized Austrian enterprise which is specialized on secure software development and security consulting.

4.3.2 General questions on information sharing

When asked about the relevance of the exchange of information security knowledge, both IS1 and IS2 answered that they deemed it very important. IS1 exchanges knowledge on a weekly basis with experts of other organizations, while IS2 does so quarterly.

For IS3 the exchange of information security knowledge with experts from other organizations is somewhat important, but for him the exchange with experts from his own organization is much more important. As a consequence IS3 hardly ever exchanges his knowledge with experts from other organizations.

The form of exchange varies, IS1 usually exchanges knowledge in the form of e-mails, text chats and electronic documents, IS2 prefers verbal exchange. IS3 prefers verbal exchange when he is able to meet other experts, but when a meeting is not possible he prefers exchange via e-mail.

When exchanging knowledge, IS1 prefers to exchange only general threat knowledge as to not reveal vulnerabilities of his organization. IS2 also exchanges general knowledge, but is also willing to share knowledge about software vulnerabilities.

IS3 said that when he decides to share his knowledge, he is willing to disclose general threat knowledge, knowledge of vulnerabilities and countermeasures as well as concrete solutions from his work environment.

When asked about the willingness to use a centralized, web-based portal to share knowledge with other security practitioners, IS1 would be willing to share his

knowledge, but has concerns about privacy issues. When anonymity of the contributions can't be guaranteed, he would not contribute, in fear of revealing critical information about security in his organization. When security mechanisms are in place and can guarantee privacy, he would share his knowledge on such a platform. IS2 would rather not contribute his own knowledge to such a platform, because he would not benefit from sharing, especially if not encouraged by his employer. On the other hand, he would use such a portal as a source for information security knowledge.

IS3 said that he would use a centralized web portal as a reference, but would contribute his knowledge only if he had a benefit from doing so. As an example he mentioned that when working on risk management, such a portal could prove to be very useful.

Regarding influencing factors in accepting knowledge from external sources, both IS1 and IS2 said that the knowledge source does influence their willingness to accept knowledge. If the source is well known, they are willing to accept this kind of knowledge. IS1 remarked, that he would require to know the source, but himself wouldn't want to appear as a knowledge source by name, for fear to reveal too much critical security information.

IS3 said that the quality of the knowledge is the main influencing factor in accepting the knowledge, especially if it coincides with his own experience and seems coherent. Generally IS3 prefers to double check the knowledge through different sources before integrating the knowledge into his work flow.

IS1, IS2 and IS3 would also accept knowledge that was rated positively by a trusted community.

IS1 finally pointed out, that using a centralized, web-based portal for information sharing would work best in a trusted community, e.g. a community stemming from personal meetings.

4.3.3 Feedback on the assignments

After performing the given assignments, the participants were asked about their impressions and opinions.

On the one hand IS1 felt that the time it took to complete the assignments was appropriate and that the web portal offered the necessary means to complete them. On the other hand IS1 pointed out that ambiguities in the used terminology made it difficult to find the best way to represent the knowledge. Especially defining the predecessor or successor threats was complex, because the direct or indirect dependencies and relations are not visible. IS1 said that it is not clear on what level a relationship should be described, for certain threats can result indirectly from another threat, which makes the modeling process overly complex.

IS1 had several suggestions regarding the efficiency of the web portal. IS1 missed the visibility of the selected language in the user settings menu, which made it clear to the user which language was selected.

When IS1 tried to select multiple entities from the *IndividualsListPortlet* in order to add new relations, this was not possible. IS1 thought that it would be very useful to add several entities at once, so that the user doesn't have to repeat the same steps over and over again.

IS1 also pointed out, that it would be helpful to be able to navigate to different entities by double clicking on them, for example on a vulnerability that is connected to a threat.

IS1 also found that some buttons were unnecessary and distracting and should be removed from certain parts of the user interface.

Regarding the layout of the web portal, IS1 thought that it was lucid and clear, but would have wished the export widget on the Home tab to be placed more prominently. He also pointed out, that there are ambiguities in the terminology used in the web portal and therefore more explanation should be offered to the users. For example the terms "Low Level Threat" and "Top Level Threat" were not clear enough in order to understand what is meant by them. IS1 said that at least some information could be offered in form of tooltips as to explain shortly to the user what is meant by these terms.

Also more explanations about the export functionality would be useful to explain users what can be done with the exported OWL files. The Home tab could for example offer information about Protégé and how an ontology can be imported into the program.

Concerning the structure of the ontology, IS1 thought that the structure was clear, but mentioned that with time it could lose its clarity, when the ontology grows and the number of entities increases.

IS1 also pointed to the fact that no meta data could be represented with the web portal, which would make the captured knowledge more useful. In the current state threats could only be represented through labels, comments and the associated relationships to other entities, but no classification or other meta data can be defined.

When asked about his willingness to contribute his own knowledge to such a web portal, IS1 said that he would only contribute if he saw clear benefits from participating. The benefits of sharing knowledge should be communicated clearly to the users in order to motivate them to participate over a longer period.

IS1 also pointed out that the question of trust between the members is essential. Only if trust is present among the participants, people will contribute their knowledge. If members of the community do not have enough trust towards the other users, they

will not share their knowledge in fear of revealing vulnerabilities which could lead to competitive disadvantages. On the other hand, if trust is given and sustained, people could benefit from sharing their knowledge with other experts.

IS2 thought that the assignments given were not too complicated, but entering the required knowledge was too much effort. It takes too much time to enter knowledge and to determine if certain entities already have existing entries.

IS2 said that in order to enhance the usability, more explanations and definitions are needed. In the current state there were many ambiguities regarding the terminology. Like IS1 before, IS2 also thought that "Low Level Threat" and "Top Level Threat" are not precise enough and should be explained in more detail to the user. Also the "exploitation degree", which describes the weight of the relation between a threat and a vulnerability, should be explained in more detail to the user, because misinterpretations are likely to happen.

Moreover IS2 mentioned several features that in his opinion would improve the usability, such as keyboard shortcuts for often used functions. Also IS2 lacked visible feedback to the user, showing which entities were already in relation to the current subject, in order to prevent double entries while adding relations to existing values. IS2 also said that it would be desirable to have the possibility to add new entities directly from the dialog used to add new relations between entities. This could help if an entity is not yet present in the knowledge base, but should be added and have a relation to the currently edited subject.

IS2 criticized that it is possible to define a threat source (e.g. deliberate or accidental) for top level threats, where according to his opinion such a definition is too restricting. The same goes for security attributes (e.g. confidentiality, integrity ...) for the low level threats, because they usually can affect several attributes and can't be restricted to one.

Another point addressed by IS2 was the possibility to define a low level threat as a successor to a top level threat, which is wrong from a modeling perspective.

IS2 also brought up the issue of the clarity of the ontology and its depiction. The ontology is presented as a list of entities, which could become confusing with rising number of entities.

IS2 had several issues with the current state of the web portal. One problem is that the target group is not clearly defined. According to his opinion, CISOs would not use the web portal due to the fact that it takes too much effort and time to add knowledge with no or little visible benefit. Especially the dynamic nature of the web portal makes it impractical for CISOs as a foundation for risk analysis.

A consultant in the field of information security would not use the portal because sharing his knowledge would take away his business foundation.

Another problem is that the benefit of participating is not clear, which is also an aspect of the not yet defined target group. This benefit has to be communicated clearly to motivate users to contribute their knowledge and to give them a justification for investing time and energy.

IS2 brought up the issue of "critical mass" of content which is required to attract users to the web portal and to make it useful for them.

IS2 found that the current system lacks a mechanism that detects double entries, preventing users from adding knowledge and entities that are already present in the ontology. For example some kind of moderator could review the knowledge base, assuring that the represented knowledge meets the quality standards.

For IS3 performing the assignments was not too difficult, though he would have liked more tooltips to explain certain functions, for example for the exploitation degree of the threat - vulnerability relation or for the tools buttons of portal widgets.

Regarding the efficiency of adding knowledge to the web portal, he suggested to add labels automatically when a new entity is created. This removes one working step that is redundant in the creation process.

IS3 felt that the layout was intuitive, but suggested that some widgets could be collapsed when not needed right away. This would save some space on the web page that could be used to enlarge more important functions. For example the widget for notes on the threats tab could be collapsed while the details form could take more space.

IS3 had also suggestions regarding the search feature when adding predecessor or successor threats. He noticed that the search results include entities from the whole ontology and not just from the class tree that is currently being edited. Here it could help if relevant results are marked according to their respective classes.

Another suggestion was related to the threat - vulnerability relation, which would be more efficient if the user could select the related entity together with the exploitation degree. This way users wouldn't have to make the additional step of changing the degree separately. Regarding the exploitation degree IS3 also said that a little explanation in the user interface would help to understand the meaning of the degree better, for example built in as a tooltip.

IS3 lacked the option to specify fixes to vulnerabilities or threats besides the ability to choose mitigating controls. IS3 said that he could describe those as comments, but this would make the purpose of comments too general. IS3 would have liked to have different options for comments, such as indicating further literature through references, website links etc.

When asked about being able to use a web portal, IS3 said that when he is working in risk management, he could use such a web portal as a reference. Regarding the contribution of his own knowledge, IS3 would require an existing, useful foundation before adding his own knowledge.

IS3 thought that the web portal could support the exchange of security knowledge between experts of different organizations, where these experts contribute and consummate knowledge at the same time. The tool could also be useful as a work of reference where current threats and vulnerabilities can be looked up.

Regarding the question about editing contributions of other users, IS3 said that he would rather not edit knowledge contributed by others, but would want to contact the user and send him suggestions. This would allow discussing a topic before a user could edit and possibly delete knowledge, adding a layer of security, preventing legit knowledge from being deleted. Alternatively IS3 suggested that an additional authority could check the submitted changes and give clearance if the contribution is valuable.

4.4 Assessment of the analysis

Through the evaluation process and the interviews conducted with information security experts several challenges in the concept of the web portal and its usability have been identified (see Table 1).

Challenge	Benefit
Rethink threat dependencies in the ontology	Creating clear hierarchies and dependencies in the ontology reduces the risk of confusion and misunderstandings
Reaching critical mass of captured knowledge	Reaching a critical mass of knowledge is crucial to attract new users to the web portal. Until it is reached use of the web portal offers little benefits
Address ambiguities in selection of terms in the ontology	Helps users to grasp the meaning of ontology and web portal elements more quickly, enhancing the work experience
Information security knowledge quality assurance	Implementing a quality assurance supports trust building that is essential for knowledge sharing
Enhance usability of web interface	Reduce the time needed to become acquainted with web portal
Define clear target group for web portal	Tailor portal to suit needs of specific target group, making portal more attractive and useful

Table 1: Challenges and expected benefits

It was shown, that especially the aspect of the target group has yet to be mapped out and clearly defined. This is important in order to be able to meet the requirements in a professional and adequate manner. Currently the target audience is too vaguely defined and therefore the actual benefits of using the web portal for information exchange can't be clearly communicated.

The evaluation process has shown that there are several possible target groups, which include software vendors, consultants, researchers, modelers and CISOs.

As one of the participants pointed out, a CISO could use the system in the process of making a risk analysis. In order to complete such an analysis, the CISO requires a

stable and comprehensible basis for the assessment and calculation. The problem here is the collaborative and highly dynamic nature of the web portal, which possibly changes this basis frequently. Therefore the CISO lacks a profound basis for decision making and loses the benefits of a well-structured approach. At the same time, if the knowledge base has a stable core that represents certified knowledge contained in best practices and standards, it can be useful as an information source for CISOs.

For example the threat tree could be managed centrally by moderators, so that on the one hand the quality of the represented knowledge is ensured and on the other hand the knowledge doesn't change as often as the rest of the entities in the ontology. Users could then for example add and edit vulnerabilities, while threats remain mostly stable. This could help CISOs somewhat so that they can rely on the modeled threat structures. It could also help if parts of the ontology are created and edited only by certified experts in order to guarantee the quality found in core parts.

Additionally CISOs would like to model their system environment in more detail than is possible in a collaborative tool, limiting the use of such a web portal further. CISOs especially require additional data about costs and consequences of vulnerabilities and countermeasures to author sound risk analyses.

IT security consultants are also a problematic target group. The problem is that in the context of a collaborative IT security ontology development, they lack the motivation to use such a web portal. Consultants primarily make money with their knowledge and would lose value if they contributed their assets without financial gain.

After successfully identifying the target group, the necessary level of detail has to be researched further so that the depth of knowledge can be adjusted to the final target group.

Generally the benefits to the users have to be specified more clearly and a unique selling point has to be defined, so that organizations and individual users are motivated to contribute their knowledge to the ontology. The aspect of motivating users and organizations to participate actively in a knowledge exchange has to be researched further.

During the evaluation it was also indicated, that certain aspects of the ontology are difficult to model and offer too much ambiguity. One of the participants pointed out that the comprehensibility of the dependencies between the different entities is not always given. For instance threats can be predecessors or successors of other

threats directly or indirectly, and this makes it difficult for users to clearly define these relations. Here it might be necessary to create clearer definitions in the ontology concept in order to be more precise in the modeling.

Also the degree specified for relations between threats and vulnerabilities has to be explained further, as some participants found the meaning unclear. Explanations can be built in as tooltips directly into the user interface or in some kind of user manual that can be offered through the web portal.

The differentiation between low and top level threats has also proven to be difficult for some participants, since the manner of classification was not clear. An explanation should make the classification clearer to the users.

The participants generally thought that at least a small amount of time is needed to become acquainted with the web portal and to be able to use it effectively. Therefore further effort has to be put into the platform to enhance the user friendliness and to make the working experience more intuitive.

It was also pointed out that the representation of the ontology classes mainly in the form of lists is only lucid as long as the number of entities is manageable. With entities increasing in number, this method of presentation could become confusing and unclear. As an alternative, some kind of visual representation was suggested; the practicability of such an approach has yet to be checked.

Another approach would be to divide the ontology into smaller parts that focus on certain business sectors in order to maintain the clarity and offer users the knowledge they require.

One of the more important points that have been found during the evaluation was the need to reach a "critical mass" of knowledge in order to attract new users to the web portal. As long as this level of information is not reached, people will not have the motivation to use the tool, because the value gained is lower than the effort that has to be put into it. This means that a certain level has to be reached right from the beginning, so that users immediately benefit from collaborating.

Another important point is that a collaborative editing of the ontology is necessary in order to divide the effort of creating a knowledge base between a large number of participants, so that a balance is reached where everyone contributes a little and gains much in return.

In order to maintain the quality of the represented knowledge, it may be necessary to have moderators regularly review the presented knowledge and remove unnecessary or incorrect data. Alternatively the tool could be based on the principle of peer-reviews and the issue of quality assurance could be left in the hands of the user community. However, this would probably only work when the user community represents a trusted environment, else the acceptance of the captured knowledge could diminish.

4.5 Outlook and future work

In this section some ideas are presented that came up during the evaluation and could be implemented in the future to enhance the functionality and usability of the web portal.

4.5.1 Selection of multiple entities

The evaluation has shown that the possibility to add multiple relations in one step would help to improve the efficiency of adding knowledge to the web portal. Future development should implement a feature that allows the users to select multiple entities for which then relations should be added.

4.5.2 Navigating ontology through double-clicks

In order to enhance the usability of the web portal, the option to navigate the ontology by double-clicking on an entity would be very useful. Such a feature would reduce the time needed to find and edit the knowledge found in the ontology.

4.5.3 Keyboard shortcuts for common functions

During the evaluation, one of the participants remarked that keyboard shortcuts for often used functions could be useful, for example to add predecessor / successor threats or similar functions.

4.5.4 Registration of new users

Currently it is only possible to use user accounts that were registered through Protégé. For the future it would be advisable to offer an option to users to register to the system. This could be implemented as a simple request message sent to the administrator or as an automatic registration requiring a confirmation by the site administrator. Another option would be to grant the freshly registered user basic rights (such as commenting) with more privileges requiring actions by the administrator.

4.5.5 Leveling user privileges based on user interaction

In order to give users incentives to contribute their knowledge to the web portal, it would be useful to have a system that analyzes the amount of contributions a user has made and adapt his privileges accordingly. This could also help to prevent that so-called "free riders" from taking advantage of other people's contributions without contributing themselves.

One possibility is to give users additional options how to work with the available knowledge. For example the option to download the ontology as an OWL file could be limited to users who have contributed at least a few times.

4.5.6 Dividing knowledge into branches for different business sectors

If the knowledge in the ontology gets too diverse, it could be favorable to branch the knowledge. There could for example be different branches corresponding to different business sectors (e.g. financial sector, media sector etc.)

4.5.7 Mark classes and individuals of special interest and enable user to download ontology only with those marked ones

Users already have the option to mark certain individuals and classes as "watched entities". It could be useful to offer users an option to mark entities of special interest, which can then be downloaded separately. This would allow users to download only the relevant concepts that they want to use on their local systems.

4.5.8 Rating of other users contributions

When the number of users is increasing, it could be useful to rate the contributions of other users in order to highlight knowledge of higher quality and to sort out impractical ones. This should help the user community to regulate itself without the need for administrators to constantly monitor contributions.

4.5.9 Voting mechanism on disputed content (with added discussion)

The Web-Protégé portal already supports attaching notes to entities and enabling the discussion of content. A voting mechanism could prove useful in cases where a consensus is hard to reach. In such a case, users could be able to vote on the disputed content to decide if and in what form it should be part of the knowledge base.

4.5.10 Add tags to certain content and build in search function to find relevant content

The use of so-called tags has become wide spread to outline a subject by keywords. This could be helpful in combination with a searching mechanism that not only looks for exact matches in the ontology.

For example a threat could be described by a number of keywords that expand the description and offer more information than the label. These keywords could then be included in search results, so that users can check the knowledge base more effectively. This would be especially important if the knowledge base grows in dimensions.

4.5.11 Add alternative names to individuals

Currently each entity has at most one name in each represented language. When the user community expands, it could come to conflicts regarding certain terms, where users would use a different label or have a different understanding of the choice of words.

In this case it could be useful to allow the definition of aliases for entities. Should a search mechanism be implemented, these could also be included in the search results.

4.5.12 Forum or messaging system to encourage discussion between users

Currently the web portal allows the attachment of notes to entities and thus supports discussions between users. This feature could be expanded, for example by giving users an additional forum to discuss contents more extensively.

5 Conclusion

As stated in the introduction to this master thesis, information systems have become very important assets to many organizations, and therefore securing the systems has become of utmost importance. This applies both for the containment of everyday risks such as failures of individual components and also for preventing malicious attacks from outside against the systems.

Knowledge on information security is an important factor to secure this resource. Many security incidents occur due to lack of knowledge about security risks, so an effective knowledge management could help to reduce certain dangers.

Together with the increasing significance of information systems, also the number and the complexity of threats and vulnerabilities are rising. The complexity of the key issues makes it more and more worthwhile to develop solutions cooperatively so that costs are distributed and benefits are enjoyed by all concerned parties.

Still, many organizations currently put an effort to solve security risks through technical solutions available on the market while ignoring the fact that security is not just a matter of technical solutions, but also includes people, processes, policies etc. In the past, mostly professionals were working with information and communication technologies, who were aware of security risks. Nowadays technology has spread so far and is being adopted by most businesses that the gap in knowledge of and skills in technology and especially security is growing.

Another main challenge concerning information security is the application of knowledge. Lots of the knowledge is available through different media like books, the internet etc., but people seldom use the sources. This can have several reasons, among them insufficient communication between users and information security experts, or a lack of motivation to extract the useful knowledge out of the available sources.

While it may seem to many users that security can be left entirely in the hands of the experts, the consequences of security breaches can be very costly for the entire organization. These consequences may be of financial nature, but can also lead to information leaks, loss of customers, loss of reputation and compromise of integrity.

One research question of this master thesis was about the ways in which sharing of knowledge on information security between organizations is possible. The hypothesis to this research question was that knowledge sharing should ideally take place over a closed joint platform, so that organizations can develop enough trust to expose crucial information and that the access to the information over the platform should be regulated to prevent misuse.

It was found that there are a number of incentives and barriers that encourage or hinder organizations to participate in information sharing. The most important incentives were of economic nature. Organizations want to benefit economically from sharing their knowledge with possible competitors.

Part of the motivation to share information is the expectation to receive knowledge of equal value. Additionally the information that is shared must be relevant to participants' concerns to ensure that participants benefit from and maintain participation.

When participants are not convinced that they gain a benefit from sharing, they won't participate. Therefore, a strong emphasis has to be put on highlighting the possible benefits for organizations.

Another major incentive and at the same time one of the most powerful barriers is the matter of trust. Almost all studies observed that trust is a crucial factor in sharing information. Participants have to be able to trust their peers with whom they share crucial and sensitive information about the state of their information security and their knowledge on the subject. This trust has to be built over time and through personal relationships. Trust can also be based on the perception that other participants have similar desires and intentions.

When trust is misused and broken, it is very difficult to rebuild it. Therefore it is most important to ensure that misuse of shared information is as difficult as it can be and that it is penalized. When information sharing between organizations takes place in a structured manner, security measures have to be implemented to keep the information safe.

There are several initiatives on sharing information security knowledge. These can be on behalf of government agencies, stemming from the private sector or from a cooperation of both the public and private sector.

These initiatives can have different goals, for example educating and raising awareness, establishing contact between the members of an information sharing community, offering assistance in responding to security incidents or disseminate warnings of security threats to a wider audience.

The second research question dealt with the ability to support knowledge sharing with a tool. The hypothesis was that a tool can provide a central platform for participating organizations over which sharing of knowledge can take place. This allows having more efficient and more structured cooperation than would be possible through classic channels like phone calls or e-mails.

It was found that the examined initiatives mostly collect data from their members, analyze it and then disseminate the found results. In many cases information exchange takes place through personal meetings, conferences etc. In such a work flow a tool could support experts participating in such initiatives to submit their knowledge and exchange information with peers in a structured manner. The advantage of such a scenario would be that it could build upon the trust already existing among expert groups.

Besides the previously mentioned initiatives there are some efforts to develop frameworks (e.g. Cybersecurity Information Exchange Framework) and tools (e.g. Mace, Parkin, & van Moorsel, 2010) that support structured information exchange.

This means that there is still much space for developing technical solutions for information security knowledge sharing. The web portal presented in this master thesis represents one approach to offer a collaborative platform for knowledge sharing. It was shown that through the use of ontologies the domain of information security can be modeled and stored in a human- and a machine-readable format, enabling both human editing and automation (e.g. for risk calculations).

Though the approach is useful, several challenges were pointed out. One such challenge is to define the target group, which might consist for example of CISOs, IT researchers, marketing professionals or a mix of different positions and professions. Depending on which audience is targeted by the tool, different aspects have to be very carefully considered in order to find the most useful solutions for the group.

Another challenge is to find the appropriate degree of detail for modeling the information security domain. While having a low degree of detail may limit the potential use of a tool for experts, modeling too much detail could limit the benefits of a collaborative tool as well, which makes finding the balance a key factor for the usefulness of a tool.

Maintaining the overview of the modeled content was also found to be a challenge. While the presentation in list form is practicable for a small number of entities, the overview is quickly lost when dealing with large numbers, making the aspect of presentation for a growing knowledge base an important factor for maintaining the usefulness of the tool.

The most important challenge a tool for knowledge sharing has to face is the aspect of motivating users to participate in a knowledge exchange. While researchers may enjoy the exchange of knowledge and ideas, organizations expect to benefit from disclosing knowledge. Therefore, as previously mentioned, concrete benefits have to be developed for the target group in order to ensure collaboration and participation in the long term.

The evaluation showed that a collaborative tool can serve as a reference for experts to look up vulnerabilities, threats and countermeasures, or could be useful to risk management experts when applied together with risk calculations. However, creating a trustful environment is crucial in order to make the collaboration work.

The evaluation also showed that before a tool can prevail, a thorough requirement analysis has to take place which identifies the needs of the target group, and a "critical mass" of knowledge has to be compiled to attract new users.

5.1 Outlook

Due to the immense importance of information and communication technologies, fixing vulnerabilities in these systems and finding countermeasures against threats is a high priority. While the systems and the threats are getting more complex, the effort put into protection often cannot be increased in the same extent. In this context the topic of sharing knowledge on information security is gaining relevance and cooperation within the IT sector holds economic benefits.

This development leads to an increasing number of initiatives with the primary focus on sharing knowledge, like for example the European Union's effort to develop the pan-European Information Sharing and Alerting System (EISAS).

Information sharing is gaining recognition as a *"powerful mechanism to better understand a constantly changing environment and learn in a holistic way about serious risks, vulnerabilities and threats, as well as solutions."*¹¹¹

Within the scope of the EISAS efforts falls the NSIE concept. This exchange is seen as *"a form of strategic partnership among key public and private stakeholders."*¹¹²

This partnership brings together governments and organizations from the private sector (such as telecommunication companies).

Besides this pan-european project there are already sector-specific information sharing partnerships between the government and the private sector in many european countries.

It can be expected that in future such initiatives will be joined by larger numbers of organizations in an effort to develop common solutions to IT security problems. This is especially true if the research on incentives and barriers is deepend. Several surveys already have dealt with the topic of motivating individuals and organizations to share their knowledge, but there are still many unanswered questions that need to be researched, for example the feasibility of economic incentives.

Here also governments can play a decisive role through relevant legislation and subsidies. Governments could encourage companies to participate in information

¹¹¹ European Network and Information Security Agency. (2009, June). *Good Practice Guide Network Security Information Exchanges*. p. 6

¹¹² Ibid.

sharing through tax allowances in the case of participation, offering potent economic incentives.

Many governments already realized the importance of information security, for example in the field of national critical infrastructure protection, and have started to support information sharing initiatives or have created efforts of their own.

On a smaller scale, the web portal presented in this master thesis has the potential to support information security experts in their everyday work. The evaluation has shown that the interface is easy to handle, though some refinements have still to be implemented. Still there are conceptual challenges that have to be addressed in future work.

During the evaluation it was also shown, that certain aspects of the ontology are difficult to model and offer too much ambiguity. For example the comprehensibility of the dependencies between the different entities is not always given.

In the process of further developing the web portal, it is important to put a stronger focus on determining the final target group. This will help to concentrate on the needs of this group and to develop a unique selling point, making the web portal more attractive to use.

At the same time incentives have to be developed to attract experts and to motivate them to contribute their knowledge.

6 References

- Aviram, A., & Tor, A. (2004). Overcoming Impediments to Information Sharing. *Alabama Law Review*, 55.2 , pp. 231-280.
- Birkenkrahe, M. (2002). How large multi-nationals manage their knowledge. *University of Auckland Business Review* , 4 (2), pp. 2-12.
- Buraga, S. C., Cojocaru, L., & Nichifor, O. C. (2006). Survey on Web Ontology Editing Tools. *Periodica Politechnica, Transactions on Automatic Control and Computer Science* .
- Donner, M. (2003). Toward a Security Ontology. *IEEE Security & Privacy* , pp. 6-7.
- European Network and Information Security Agency. (2009, June). *Good Practice Guide Network Security Information Exchanges*. Retrieved January 17, 2012, from http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide/at_download/fullReport
- European Network and Information Security Agency. (2010, September). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. Retrieved January 17, 2012, from http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing/at_download/fullReport
- Fenz, S., & Ekelhart, A. (2009). Formalizing Information Security Knowledge. ASIACCS. Sydney, Australia: ACM.
- Fenz, S., Parkin, S., & van Moorsel, A. (2011). A Community Knowledge Base for IT Security. *IT Professional* , 13 (3), pp. 24-30.
- Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research* , 16 (2), 186-208.
- Glaser, T., & Pallas, F. (2007). *Information Security and Knowledge Management: Solutions Through Analogies?* Berlin: Technische Universität Berlin.
- Information Assurance Advisory Council. (2002). *Sharing is Protecting - A Review of Information Sharing*. Retrieved January 17, 2012, from <http://www.warp.gov.uk/downloads/IAAC%20NISCC%20Sharing%20is%20Protecting%20v21.pdf>
- International Telecommunication Union - Study Group 17. (2010, December 8). *Draft Recommendation ITU-T X.1500*. Retrieved January 13, 2012, from The Internet Engineering Task Force: http://www.ietf.org/mail-archive/web/scap_interest/current/doc9OXValF1qq.doc

- Kesh, S., & Ratnasingam, P. (2007, July). A Knowledge Architecture for IT Security. *Communications of the ACM* , 50 (7), pp. 103-108.
- Knights, M. (2009, January 29). *Security breaches cost \$1 trillion last year*. Retrieved February 4, 2012, from IT Pro: <http://www.itpro.co.uk/609689/security-breaches-cost-1-trillion-last-year>
- Mace, J. C., Parkin, S., & van Moorsel, A. (2010). A Collaborative Ontology Development Tool for Information Security Managers. *Computer-Human Interaction for Management of Information Technology*. San Jose, California: ACM.
- Martimiano, L. A., & Moreira, E. (2006). The Evaluation Process of a Computer Security Incident Ontology. *2nd Workshop on Ontologies and their Applications (WONTO 2006)*. Sao Paulo.
- McAfee, Inc. (2009). *Unsecured Economies: Protecting Vital Information*. Santa Clara: McAfee, Inc.
- Messenger, M. (2006, February 13). *Cyber-security: Why would I tell you? Research briefing*. Retrieved January 17, 2012, from http://archive.nyu.edu/bitstream/2451/15007/2/Infosec_ISR_Messenger.pdf
- Mittal, Y. K., Roy, S., & Saxena, M. (2010, November). A Knowledge Management Model to Improve Information Security. *International Journal of Computer Science Issues* , 7 (6).
- Mittal, Y. K., Roy, S., & Saxena, M. (2010, November). Role of Management in Enhancing Information Security. *International Journal of Computer Science Issues* , 7 (6), pp. 320-324.
- Parkin, S. E., van Moorsel, A., & Coles, R. (2009). An Information Security Ontology Incorporating Human-Behavioural Implications. *International Conference on Security of Information and Networks* (pp. 46-55). Gazimaguse, North Cyprus: ACM.
- PricewaterhouseCoopers. (2010). *Information Security Breaches Survey 2010 - Technical Report*. Retrieved January 17, 2012, from http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf
- Rutkowski, A. (2011). Enhancing Security for Next Generation Networks and Cloud Computing. *ETSI Workshop*. Sophia Antipolis.
- Rutkowski, A., Kadobayashi, Y., Furey, I., Rajnovic, D., Martin, R., & Takahashi, T. (2010, October). CYBEX - The Cybersecurity Information Exchange Framework (X.1500). *ACM SIGCOMM Computer Communication Review* , Volume 40 (5), pp. 59-64.
- Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). *Human Vulnerabilities in Security Systems*. Retrieved January 17, 2012,

from

<http://hornbeam.cs.ucl.ac.uk/hcs/publications/HFWG%20White%20Paper%20final.pdf>

Schumacher, M. (2003). Toward a Security Core Ontology. In M. Schumacher, *Security Engineering with Patterns* (pp. 87-96). Berlin: Springer-Verlag.

Singhal, A., & Wijesekera, D. (2010). Ontologies for Modeling Enterprise Level Security Metrics. *Cyber Security and Information Intelligence Research Workshop*. Oak Ridge, Tennessee: ACM.

Stepanova, D., Parkin, S. E., & van Moorsel, A. (2009). A Knowledge Base for justified Information Security Decision-Making. *International Conference on Software and Data Technologies*. Sofia, Bulgaria.

Takahashi, T., Kadobayashi, Y., & Fujiwara, H. (2010). Ontological Approach toward Cybersecurity in Cloud Computing. *International Conference on Security of Information and Networks* (pp. 100-109). Taganrog: ACM.

Tsoumas, B., Dritsas, S., & Gritzalis, D. (2005). An Ontology-Based Approach to Information Systems Security Management. In V. Gorodetsky, I. Kotenko, & V. Skormin, *Computer Network Security* (Vol. 3685, pp. 151-164). Springer Berlin / Heidelberg.

Tudorache, T., Vendetti, J., & Noy, N. F. (2008). Web-Protege: A Lightweight OWL Ontology Editor for the Web. *OWL: Experiences and Directions*. Karlsruhe, Germany.

United States General Accounting Office. (2004). *Critical Infrastructure protection. Establishing Effective Information Sharing with Infrastructure Sectors*. Retrieved January 17, 2012, from <http://www.gao.gov/new.items/d04699t.pdf>

United States General Accounting Office. (2001). *Information Sharing. Practices that can benefit Critical Infrastructure Protection*. Retrieved January 17, 2012, from <http://www.gao.gov/new.items/d0224.pdf>

Vlacheas, P. T., Stavroulaki, V., Demestichas, P., Cadzow, S., Ikononou, D., & Gorniak, S. (2011). *Ontology and Taxonomy of Resilience*. Retrieved January 17, 2012, from <http://www.enisa.europa.eu/act/it/technology-for-resilience/ontology/resontax-draft>

Vorobiev, A., & Bekmamedova, N. (2010, February). An Ontology-Driven Approach Applied to Information Security. *Journal of Research and Practice in Information Technology*, 42 (1), pp. 61-76.

WebProtege Admin Guide. (n.d.). Retrieved November 01, 2011, from Protege Wiki: <http://protegewiki.stanford.edu/wiki/WebProtegeAdminGuide>

WebProtege Layout Configuration. (n.d.). Retrieved October 16, 2011, from Protege Wiki: <http://protegewiki.stanford.edu/wiki/WebProtegeLayoutConfig>

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). Human, Organizational and Technological Challenges of Implementing IT Security in Organizations. *Information Management & Computer Security* , 17 (1), pp. 4-19.

Working with the Database Backend in OWL. (n.d.). Retrieved November 01, 2011, from Protege Wiki:
http://protegewiki.stanford.edu/wiki/Working_with_the_Database_Backend_in_OWL