2012 Seventh International Conference on Availability, Reliability and Security

Challenges of Web-based Information Security Knowledge Sharing

Daniel Feledi and Stefan Fenz
Vienna University of Technology and SBA Research
Email: daniel.feledi@student.tuwien.ac.at, sfenz@sba-research.org

***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 paper examines how machine-readable information security knowledge can be shared between different organizations on the basis of a web portal utilizing Web-Protégé. It can be 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). The evaluation of the web portal has shown that the most important challenge a tool for knowledge sharing has to face is the aspect of motivating users to participate in a knowledge exchange.**

***Index Terms*—information security, knowledge sharing, security ontology, web-based collaboration**

I. 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.*[1]"
In a study conducted in 2008 "*McAfee projected that companies worldwide lost more than $1 trillion [...]* [6]" 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'* [8]"
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.
To be able to approach such challenges in a professional manner, experts have to collect knowledge on information security and potential risks and have to create their own solutions to reduce them. Therefore, it would be of advantage to allow information security knowledge sharing between experts, so that the same solutions are not 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. Currently organizations are comparing solutions with other organizations, but there is no unifying system with a widespread basis which supports knowledge sharing in a formal and structured way. This paper will present a web portal based on Web-Protégé, aiming to offer a tool for the structured sharing of information security knowledge.

A. Research question

The research question this paper tries to answer is whether and in which form a tool can support information security knowledge sharing between organizations. The working hypothesis is that a tool can provide a central platform for participating organizations over which a 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. In the following sections we will discuss the functionality and the evaluation of an existing information security knowledge sharing portal based on Web-Protégé that aims to offer such a centralized platform.

II. Web portal

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

978-0-7695-4775-6/12 $26.00 © 2012 IEEE
DOI 10.1109/ARES.2012.59

effort is divided among a larger number of participants.

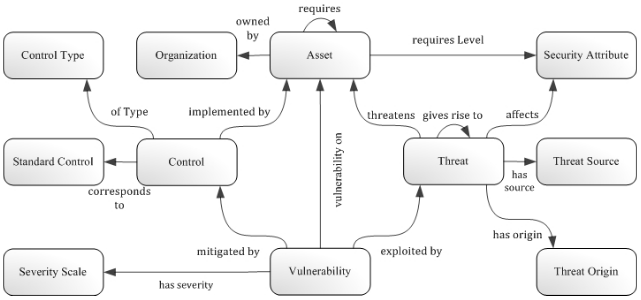


Fig. 1. Security Ontology (Fenz & Ekelhart, 2009, p.2)

The security ontology on which the portal is based on captures different concepts and interrelations within the information security domain. As shown in Figure 1 above, the security ontology consists of several classes, of which the main classes will be described in the following.

A. Security Ontology

1) The Asset Class: The concept ”asset” refers to 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.

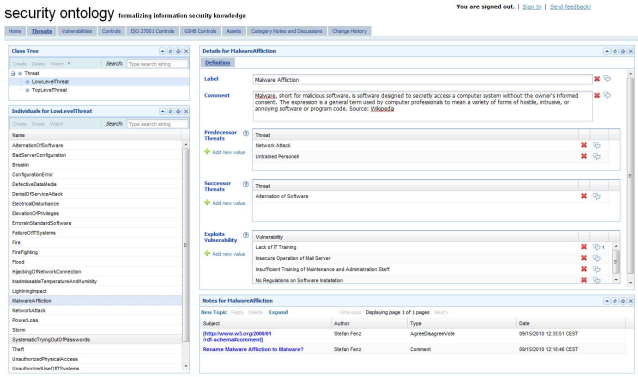
2) The Control Class: When implemented correctly, controls can mitigate vulnerabilities and protect the affected assets. Controls can have preventive, corrective, deterrent, recovery or detective measures, depending on the control type. Controls are derived from and correspond to best-practice and information security standard controls (e.g., ISO 27001)

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

4) The Vulnerability Class: Vulnerabilities are exploited by threats in the form of physical, technical or administrative weaknesses. How severe an exploit can be is determined by the vulnerability severity (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.

B. Web portal

In order to enable collaborative, web-based security ontology editing, a web portal based on Web-Protégé[1] was created (cf. [4]). In the following section a short introduction to the web portal will be given. 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 (cf. [4]). 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.


security ontology formalizing information security knowledge
You are signed out. | Sign In | Send feedback!
Home
Threats
Vulnerabilities
Controls
ISO 27001 Controls
GSHB Controls
Assets
Category Notes and Discussions
Change History
Class Tree
Create
Delete
Watch
Search:
Type search string
Individuals for LowLevelThreat
Details for MalwareAffliction
Definition
Add new value
Notes for MalwareAffliction
New Topic
Reply
Delete
Expand
<Previous
Next>

Threat
- LowLevelThreat
- TopLevelThreat

Name
AlternationOfSoftware
BadServerConfiguration
BreakIn
ConfigurationError
DefectiveDataMedia
DenialOfServiceAttack
ElectricalDisturbance
ElevationOfPrivileges
ErrorsInStandardSoftware
FailureOfITSystems
Fire
FireFighting
Flood
HijackingOfNetworkConnection
InadmissableTemperatureAndHumidity
LightningImpact
MalwareAffliction
NetworkAttack
PowerLoss
Storm
SystematicTryingOutOfPasswords
Theft
UnauthorizedPhysicalAccess
UnauthorizedUseOfITSystems

Label: Malware Affliction

Comment: Malware, short for malicious software, is software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Source: Wikipedia

Predecessor Threats

Threat
Network Attack
Untrained Personell

Successor Threats

Threat
Alternation of Software

Exploits Vulnerability

Vulnerability
Lack of IT Training
Insecure Operation of Mail Server
Insufficient Training of Maintenance and Administration Staff
No Regulations on Software Installation

Displaying page 1 of 1 pages

Subject	Author	Type	Date
[http://www.w3.org/2000/01/rdf-schema#comment]	Stefan Fenz	AgreeDisagreeVote	09/15/2010 12:35:51 CEST
Rename Malware Affliction to Malware?	Stefan Fenz	Comment	09/15/2010 12:16:46 CEST

Fig. 2. Screenshot of the web portal (URL: sec.sba-research.org)

Figure 2 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.

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.)

C. Identified challenges

In a preliminary evaluation of the web portal several challenges have been identified that had to be addressed. Among these were the missing possibility to connect existing individuals from the ontology, the lacking support for multiple languages and the limited options to send user feedback. Another missing feature was the definition of the severity of vulnerabilities, which is important in order to assess the impact of a vulnerability.
These challenges were addressed by the implementation of several extensions, which will be described in the following section.

[1] URL: sec.sba-research.org

D. Extensions

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.

Attributes such as threat source, threat origin, security attribute and control type were incorporated in order to improve the expressiveness of the ontology and to give users more options to describe threats or controls.

A feedback widget was implemented 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 implemented in order to attract users from different countries and regions, enabling them to capture and discuss information security knowledge in their own languages. 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 implemented to serve as an incentive for participants, since 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.

III. Evaluation

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.

A. Methodology

For the evaluation we selected three experts with at least five years of information security expertise. Expert 1 (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. Expert 2 (IS2) is a security specialist with 5 years of experience and is working in the IT security consulting sector. Expert 3 (IS3) works as a security specialist at a small-sized Austrian enterprise which is specialized on secure software development and security consulting. The evaluation process is structured in three phases:

- Phase 1: 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 (risk and compliance management), (ii) an overview of the captured concepts, and (iii) a general overview of the main functions of the web portal.
- Phase 2: Within the second phase we assigned three assignments to the participants (adding new knowledge, editing existing knowledge, and exporting knowledge). Only a brief introduction to the web portal was given to evaluate how intuitive the interface is.
- Phase 3: Within the third phase we gathered user impressions and opinions about the web portal by structured and open questionnaires.

B. Results

After performing the given assignments (adding new knowledge, editing existing knowledge, and exporting knowledge), the participants were asked about their impressions and opinions. In the following we provide a qualitative overview of the results:

1) IS1 Feedback: 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. 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 explanation 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.

2) IS2 Feedback: 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.

3) IS3 Feedback: 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.

C. Summary

The challenges that were derived from the evaluation are explained in this section, and have additionally been summarized in Table 1 along with their 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.

Challenge	Benefit
Define clear target group	Tailor portal to suit needs of specific target group, making portal more attractive and useful
Enhance usability	Reduce the time needed to become acquainted with web portal
Address ambiguities in term selection	Helps users to grasp the meaning of ontology and web portal elements more quickly, enhancing the work experience
Rethink threat dependencies	Creating clear hierarchies and dependencies in the ontology reduces the risk of confusion and misunderstandings
Reaching critical mass	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
Quality assurance	Implementing a quality assurance supports trust building that is essential for knowledge sharing

TABLE I
EVALUATION RESULTS

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 tool tips 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.

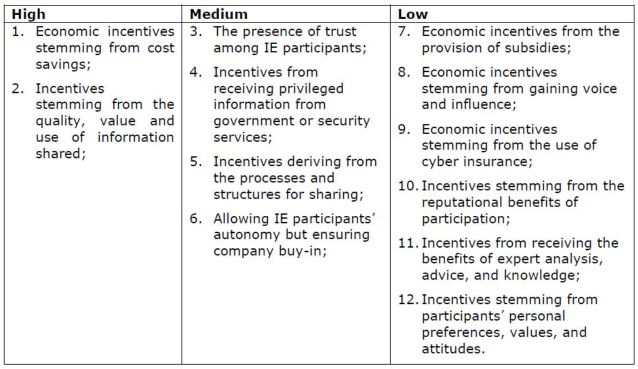
It was also pointed out that the representation of the ontology classes mainly in the form of lists is only lucid as long as the number of entities is manageable. With entities increasing in number, this method of presentation could become confusing and unclear. As an alternative, some kind of visual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

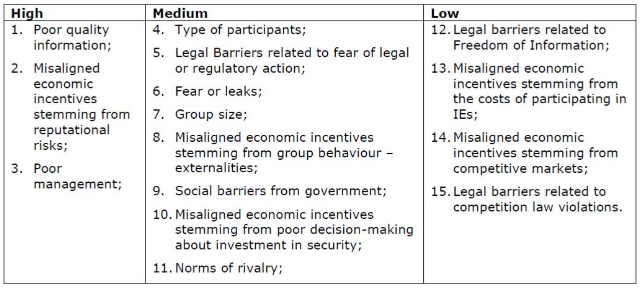
IV. Related Research

In (ENISA, 2010) incentives and barriers to information security sharing were identified and summarized (see Figure 3 and 4) [2].



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.

Fig. 3. Incentives for Information Sharing (ENISA, 2010, p. 13)



High	Medium	Low
1. Poor quality information; 2. Misaligned economic incentives stemming from reputational risks; 3. Poor management;	4. Type of participants; 5. Legal Barriers related to fear of legal or regulatory action; 6. Fear or leaks; 7. Group size; 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;	12. Legal barriers related to Freedom of Information; 13. Misaligned economic incentives stemming from the costs of participating in IEs; 14. Misaligned economic incentives stemming from competitive markets; 15. Legal barriers related to competition law violations.

Fig. 4. Barriers for participation (ENISA, 2010, p. 25)

The economic incentives are the result of cost savings, which can result *”from quicker reaction to threats, vulnerabilities and attacks, or from anticipating network failures”*. 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 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. Another medium ranked incentive is the possibility to receive privileged information from government or security services, which is not available from other sources. 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. 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. 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”*.

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.

Aside from incentives that encourage participation in an information exchange, there are of course also barriers. ENISA (2010) identified the low quality of shared information as the most significant barrier. The submission of threat, incident and vulnerability data requires the *”assured confidentiality and* *elaborate safeguards against inadvertent disclosure"*. 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. 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. 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"*.

Figure 5 summarizes the incentives and barriers for information security sharing that have been identified in ENISA (2010).

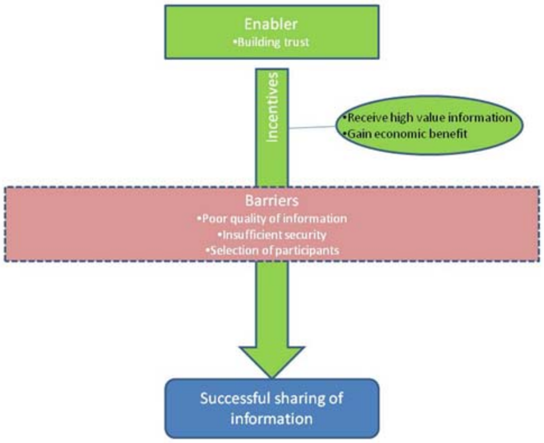

Enabler
•Building trust
Incentives
•Receive high value information
•Gain economic benefit
Barriers
•Poor quality of information
•Insufficient security
•Selection of participants
Successful sharing of information

Fig. 5. Overview of the most important enablers, incentives and barriers

From a technical perspective 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."* [7] 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."* [7] 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."* [7]

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"* [10]. 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.

Fenz (2009) developed a security ontology representing domains such as threats, controls, assets and vulnerabilities in order to formalize information security knowledge. In (Fenz, 2011) an information security knowledge management portal is presented, which uses Web-Protégé to enable collaborative editing of the knowledge captured in the underlying ontology. This web portal was the foundation for the work in this paper.

V. Conclusion

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 barrier 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 is still much space for developing technical solutions for information security knowledge sharing. The web portal presented in this paper 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 could be 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.

VI. Outlook

The web portal presented in this paper 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.

References

[1] European Network and Information Security Agency, *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/* June 2009

[2] European Network and Information Security Agency, *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/* September 2010

[3] Fenz, S., & Ekelhart, A. *Formalizing Information Security Knowledge*. ASIACCS. Sydney, Australia: ACM, 2009

[4] Fenz, S., Parkin, S., & van Moorsel, A. *A Community Knowledge Base for IT Security*. IT Professional , 13 (3), pp. 24-30, 2011

[5] Glaser, T., & Pallas, F. *Information Security and Knowledge Management: Solutions Through Analogies?*, Berlin: Technische Universitt Berlin, 2007

[6] Knights, M., *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*, 2009, January 29

[7] Mace, J. C., Parkin, S., & van Moorsel, A. *A Collaborative Ontology Development Tool for Information Security Managers. Computer-Human Interaction for Management of Information Technology.* San Jose, California: ACM, 2010

[8] McAfee, Inc. *Unsecured Economies: Protecting Vital Information.* Santa Clara: McAfee, Inc, 2009.

[9] Parkin, S. E., van Moorsel, A., & Coles, R. *An Information Security Ontology Incorporating Human-Behavioural Implications*. International Conference on Security of Information and Networks (pp. 46-55). Gazimaguse, North Cyprus: ACM, 2009

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