A Community Project to create a Shared Open Information Security Knowledge Base

Aad van Moorsel and Simon Parkin, Newcastle University
Stefan Fenz, SBA, Austria

Societal Grand Challenge: Security

Abstract
Organizations small and large are struggling to effectively manage the security of their information and computing systems. One of the main challenges is that the environment in which decisions need to be made is exceedingly complex and continuously changing: technology changes, new vulnerabilities appear, business priorities may change, laws may be altered and employee behaviour is dependent on all these and other circumstances. The TSB funded 'Trust Economics' project[1] is creating scientifically grounded modelling tools to allow for objective information security decision making in this environment. However, a serious challenge exists in making this methodology widely accessible and in assuring it is informed by the latest insights and information about vulnerabilities and trade-offs. Moreover, it would be desirable if organizations can learn from each other so that decisions do not need to be decided separately in every organization. Therefore, we propose to start a community project for the sharing of information security knowledge. We sketch the implementation in this vision statement, and discuss some of the many pitfalls that need to be avoided for a shared information security knowledge base to become reality.

The Idea and its Implementation

We propose to pool the efforts of researcher, security officers and others to create a user-community knowledge base. This acts as a completely open and shared approach to the creation and management of information security management knowledge. This formalized knowledge can be made available to human users and reasoning engines alike, and extended with additional insights and research findings from various sources. As well as encouraging wider contribution, use of the knowledge base would serve to verify and improve the knowledge it contains, in turn making it more reliable and thereby promoting wider use.

By relating and formalizing knowledge content, users of the knowledge base will be able to traverse between different types of advice from different disciplines, and at the same time focus on those aspects of information security most pertinent to their organization's needs. A consistent and unambiguous underlying knowledge classification approach systematizes the addition and subsequent communication of new and disparate sources of advice and their inherent vocabularies.

A formalized knowledge base can inform many aspects of information security management, such as risk management, IT-security investment decision making, compliance checks, and awareness training. It can also provide an opportunity for security managers to extend their existing knowledge, by investigating interconnected knowledge relating the various technical, human, legal, regulatory and business aspects of information security management. A community knowledge base allows us to share and leverage our own and each other's insights, making information security management decisions more robust.

[1] TSB grant P0007E, which also supports this work. A description of the Trust Economics project can be found in R. Coles *et al., "Trust Economics Feasibility Study"*, Dependable Systems and Networks, pp. A45—A50, 2008.

Existing information security ontologies act as a starting point and semantic Wikis such as Semantic MediaWiki [8] are used to communicate ontology content to users and facilitate the contribution of knowledge. Web 2.0 features such as ranking systems or comments can potentially transform an individual's opinion to evidence that can be used by the entire community. Similar to Wikipedia, the entire knowledge base should be open and freely available to the community, perhaps using public-private-partnership models to finance its maintenance and development. The most important point in the sensitive information security domain is to established trust among the contributors of the deployed knowledge base. There are several ideas on how to do this, but these are still under discussion.

Challenges

To implement the shared and open information security knowledge base, we need a methodology to collaboratively manage and extend the knowledge base. Such a methodology has to consider at least three different aspects: social, technical, and business.

The social aspect has to deal with the following questions: How is information security knowledge shared? Who is willing to share his/her knowledge, and under which circumstances? How can we get from individual opinions to global evidence? How should potential conflicts in obtained knowledge be handled? How can we incorporate confidential organization-specific knowledge and how can we securely separate it from the public knowledge body? Moreover, we must ensure that contributing to the knowledge base does not create new vulnerabilities (e.g. appearing to help an attacker to understand the weaknesses of a particular organization)! All these issues form potential show stoppers. We believe we cannot know the answers to these questions until we try to build such a system, but would welcome early discussions and opinions.

The technical aspect deals with knowledge annotation and collection. How should the knowledge be annotated and represented so that it can be reasoned over to make it applicable to the wider community? One needs to record the attributes of knowledge contributors (such as their organization type, industry type, size of the organization and security attributes of the working culture). Alternatively, data captured from the web may serve as input to the knowledge base, and the question is how to automate this while maintaining quality control. In any case, technologically we can deal with these problems.

From a business perspective we have to assess the expectations of potential contributors to the knowledge base. What are organizations obliged to contribute and how can we encourage contribution? The needs of the business must be clearly identified and considered during design of the knowledge model and the corresponding knowledge base. Knowledge may be used to inform real-time management of the IT security infrastructure (e.g. using up-to-date vulnerability data and associated risk assessment knowledge when scanning the network for problems). Strategic IT decisions, such as reviewing the ISO 27001 compliance of the IT environment, may utilize knowledge derived from and relating to established information security standards to identify appropriate controls.

Conclusion

In this short vision statement, related to the BCS security societal grand challenge, we propose a community project to build a shared, open knowledge base for information security, such that organizations do not have to reinvent the information security wheel in each organization separately. Whether such a solution can be effectively implemented and has a chance to gain acceptance remains to be seen—insight in this question would benefit from open early discussions.