A KNOWLEDGE BASE FOR JUSTIFIED INFORMATION SECURITY DECISION-MAKING

Daria Stepanova, Simon E. Parkin and Aad van Moorsel
School of Computing Science, Newcastle University, Newcastle-upon-Tyne, U.K.

Keywords: Information security, Ontology, Knowledge base, Human-behavioural factors.

Abstract: The majority of modern-day companies store commercially sensitive and valuable information assets in digital form. It is essential for the Chief Information Security Officer (CISO) within an organisation to ensure that such information is adequately protected. External standards exist to advise CISOs on how to secure information, but these are essentially "one-size-fits-all". Furthermore they do not consider the human-behavioural aspects that determine the impact of security controls upon employees, or how security controls can be best deployed to manage insecure employee behaviour. CISOs require more information than they are currently provided with to justify their information security management decisions.
Here we present a knowledge base and accompanying user interface. The knowledge base represents key structural components of the ISO27002 security standard, formally relating them to one another. This empowers CISOs to understand how different security measures impact upon each other. It also considers how human-behavioural factors can be associated with these concepts. The accompanying user interface provides a means to present formalised information security concepts to CISOs. This paper describes the development of the knowledge base and user interface, highlighting and discussing key challenges and how they were resolved.

1 INTRODUCTION

Large organisations increasingly follow information security standards when managing their assets (e.g. the ISO27K series, such as ISO 27002 (BS, 2005)). Such standards offer only management-level recommendations, which must be adjusted to the specific requirements of individual companies. However, Chief Information Security Officers (CISOs) are often not provided with a complete picture of the organisation's operational requirements and how IT impacts upon them (C. Alberts, 2004).

Within this paper we relate knowledge from standards to the consideration of employee behaviour within information security management. CISOs cannot afford to ignore the human element within the organisation (KTN, 2007). Organisations must cultivate an awareness of the human-behavioural implications of their information security decisions, and the CISO is best positioned to achieve this. An example would be acknowledging both a need for employees to use removable storage devices and the potential for employees to lose these devices, and mandating that all storage devices be encrypted to protect valuable data in such an event. Understanding the usability needs of employees should be a priority for CISOs (Skidmore, 2003), as it can help in identifying and managing persistent clashes between security mechanisms and end-users (ISACA, 2009).

This paper is focused on structuring knowledge from information security standards so as to provide additional benefits. For this we develop a knowledge base application to encapsulate facts and processes relating to information security. We build upon the static content of an information security standard by identifying relationships between the different information security concepts within. We then associate these concepts with additional information relating to the work behaviours of staff.

The knowledge base is built on an information model (or *ontology*), populated with management recommendations from multiple information security standards. We also developed a user interface application driven by the knowledge base content.

Discussion of the ontology and user interface follows in Sections 2 and 3 respectively. Related work is described in Section 4, with concluding remarks in Section 5.

Stepanova D., Parkin S. and Moorsel A. (2009).
A KNOWLEDGE BASE FOR JUSTIFIED INFORMATION SECURITY DECISION-MAKING.
In *Proceedings of the 4th International Conference on Software and Data Technologies*, pages 326-331
DOI: 10.5220/0002256703260331

2 KNOWLEDGE BASE DESIGN

CISOs require more information to inform their information security management decisions. We refer specifically to information relating to human-behavioural factors within the workplace, and how human behaviour can influence or be influenced by information security measures. There is then a requirement to associate information relating to human-behavioural factors with existing decision-making criteria. In this case the existing criteria may be information security standards, as these are often implemented to provide a measure of an organisation's security competence.

A second requirement is to present existing and additional (i.e. human-behavioural and usability) management criteria to a CISO effectively. This is addressed in the user interface (Section 3). Any further knowledge derived from or associated with information security management content must be presented logically if it is to assist the decision-making process.

2.1 The Need for an Ontology

To create an information security knowledge base it is essential to define the concepts to be represented, and the relationships that exist between them. For this we chose to develop an ontology, which would be appropriate for a number of reasons (as stated elsewhere in (S. E. Parkin, 2009):

- By providing a taxonomy of information security terminology, there is scope for security engineers to broaden their knowledge of related concepts.
- An ontology facilitates interoperability, not least between different assessment methodologies or software tools. This can potentially generate new knowledge.
- To represent terminology in an ontology it is necessary to reduce a diverse array of terms, concepts and relations into a refined, structured information model. This makes precise any knowledge and process information.

2.2 Scope of the Knowledge Base

Our work uses the ISO27002 standard as a context, as an example of a framework that CISOs often work within, and with which we could associate human-behavioural factors. The University Colleges and Information Systems Association (UCISA) Information Security Toolkit (developed by the University of Reading) (UCISA, 2005) was chosen as an additional source of information. The UCISA toolkit differs in that it is targeted towards educational institutions. As the UCISA standard references and expands upon the BS7799 standard (a predecessor to ISO27002), using these two standards together allows us to investigate ways of representing knowledge from similar sources.

The content of the knowledge base was restricted to guidelines relating to employees' use of removable data storage devices (e.g., to transfer work to client premises for presentation). This allowed us to build on previous findings that have shown a need to consider human-behavioural factors when securing information on removable USB storage devices (A. Beautement, 2008),(R. Coles, 2008).

2.3 Approach to Ontology Development

We followed recommendations for ontology design as found in (N. F. Noy, 2000). The structure of the ontology was also inspired in part by the work of Fenz et al (S. Fenz, 2007), who developed an ontology incorporating ISO27001/2 content (discussed further in Section 4).

The ontology was developed using the Ontology Web Language (OWL) (W3C, 2004). We chose OWL as it is extensible and well-supported. By following ontology design recommendations and encoding our ontology in an ontology language we provide well-structured, meaningful information security knowledge. We used the Protégé Ontology Editor application (Stanford, 2009) to construct the ontology and enter data.

2.4 Overview of Knowledge Base Components

The content of the ontology is introduced in Figure 1. For brevity the Asset definitions are restricted to those relating to removable media. The components of the ontology are described in the following sections.

2.4.1 Asset

An `Asset` represents something of value to an organisation which may require protection. We focus on 'Removable Device' `Assets`. This includes removable USB storage devices (USB sticks, external hard drives etc.), as well as write-once and rewritable CDs and DVDs.

2.4.2 Source

A `Source` represents the standard from which guidelines are taken. We represent two `Sources`, ISO27002 and the UCISA Toolkit. Each standard has corresponding subclasses that describe its structure. The

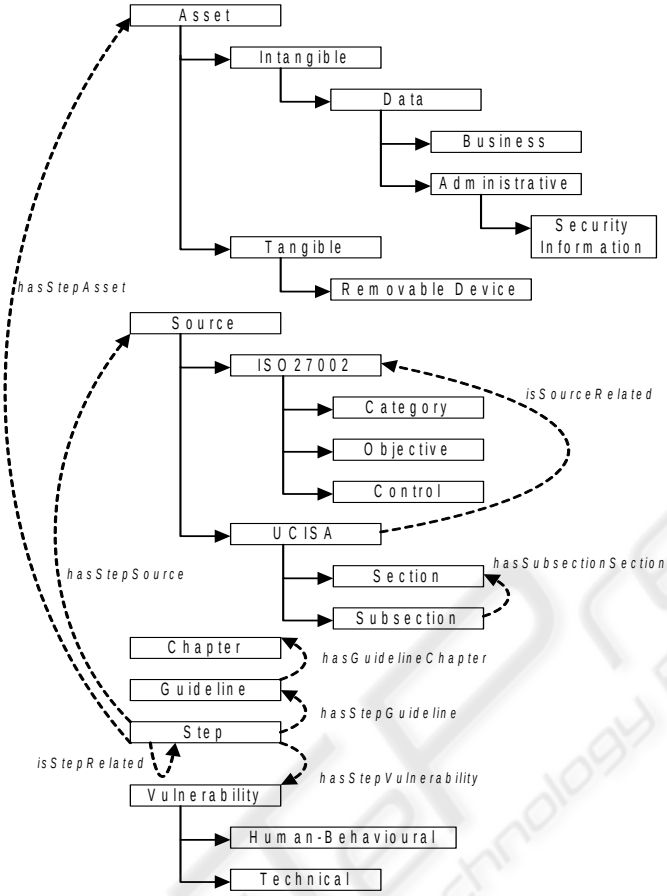

Figure 1: Overview of the ontology.

`Source` class allows representation of different information sources, so it is possible to add additional standards in the future (owing to the extensibility of an ontology).

To facilitate integration of different `Sources`, a unifying knowledge hierarchy was created. This structure consists of the `Chapter`, `Guideline` and `Step` classes (where a `Step` is a refinement of part of a `Guideline`). Content relating to use of removable storage devices was extracted from the standards and arranged according to this hierarchy via the '`hasStepSource`' relation. The '`isStepRelated`' relation identifies links between (potentially previously non-associated) `Steps`.

Once concrete `Guideline` and `Step` definitions have been created, it is possible to identify the `Assets` that specific recommendations refer to (via the '`hasStepAsset`' relation).

2.4.3 Vulnerability

Each `Asset` can have additional knowledge attached to it, as per the established information security paradigm that *"an Asset may expose a weakness or Vulnerability which can potentially be exploited"*, via the '`hasStepVulnerability`' relation. We can then relate human-behavioural vulnerabilities to the content of a standard in a structured manner.

In our ontology a `Vulnerability` may be either `Technical` (i.e. relating to the information security hardware/software infrastructure) or `Human-Behavioural` (i.e. part of an activity or process that requires the interaction of a person). The separation of technical and human factors within a standards framework provides CISOs with a formalised perspective on behavioural issues and their relevance to existing IS management concerns.

As an example, a `Step` "Security Media Storage" `hasStepAsset` {"USB", "CD"}, and `hasStepVulnerability` "NoProtectionOfUnauthorisedAccess".

We developed `Vulnerability` definitions associated with each guideline and links between guidelines by decomposing the ISO27002 and UCISA standards. We also consulted experts within a large IT consultancy and reviewed related research documen-

tation. Ideally development of further ontology content would be achieved through consultation with experienced IS professionals and existing research in this way. This approach also proved effective in the work in (S. E. Parkin, 2009), wherein an information security ontology incorporating human-behavioural factors was developed and content produced to represent management considerations in an organisation's password authentication policy.

3 KNOWLEDGE BASE INTERFACE APPLICATION

A user interface was developed for CISOs to access the knowledge base. We considered the usability requirements of CISOs by building a system that aligns the knowledge base and the representation of that knowledge to the user. Through consultation with a CISO within a large financial organisation we were able to structure and illustrate the relationships between ontology classes in a more logical manner. The main interface window is shown in Figure 2.

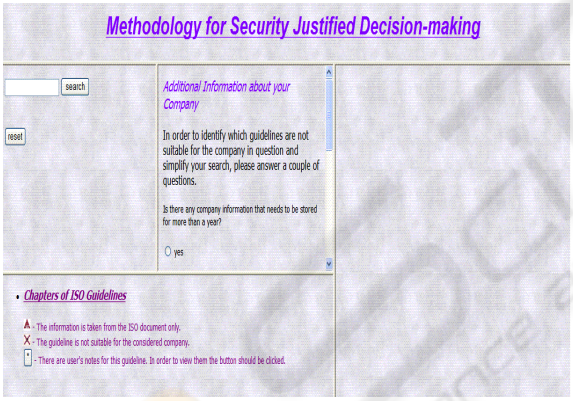

Figure 2: Overview of Knowledge Base user interface application.

In Figure 2 a number of features can be seen:

- Search Window (Top-Left): users can search for content featuring specific keywords, instead of traversing the guidelines in search of it.
- Questionnaire (Middle): a CISO can answer specialised management questions. The answers are used to refine the guidelines that apply to the organisation.
- Guideline Hierarchy (Bottom): content from standards is arranged in a hierarchy to enable simple navigation. Our example content follows the structure of the ISO27002 standard. Content should have a logical structure and indicate its source to aid in auditing and compliance processes.
- Guideline Information (Right): provides specific guideline content, as well as associated `Asset` and `Vulnerability` information. This is where human-behavioural factors are linked to individual guidelines.

We developed the user interface using HTML, JavaScript and jOWL (Decraene, 2009). This provided a lightweight, browser-based application that could be accessed across various systems and with limited resource requirements.

3.1 Accessing Knowledge Base Content

The simplest way to view content is to follow the guideline hierarchy to an individual guideline. Each guideline link provides a tool-tip text box indicating the source.

Use of the hierarchy is appropriate for users who know which guidelines they wish to view, however other approaches to finding knowledge base content are also useful. Users may be assisted through use of the search engine (as shown in Figure 2), which finds mention of entered `Asset` names within guideline `Steps`. We assume that a user would use similar terminology to the `Source` standards. However the knowledge base application can use synonyms to associate keywords with specific guidelines (e.g., if "portable storage device" and "removable media" refer to the same `Asset`).

Ontology content can be tailored to a particular organisation by use of the questionnaire shown in Figure 2 (which here focuses on removable storage device policy). An example would be to ask a CISO if they store data on removable devices for more than a year at a time (in which case a particular ISO27002 guideline applies). The questionnaire identifies both guidelines that are applicable to the organisation and those that can be ignored.

3.2 Presentation of Guideline Content

When a user has chosen a specific guideline to view, content is presented as in Figure 3.

Content for each guideline is divided into:

- Content: original text from a `Guideline` or `Step`.
- Vulnerability: the `Vulnerability` types associated with the guideline.
- Links: cross-references to other stored guidelines.
- Info: additional related knowledge from the `Source` or other sources such as modelling tools (see Section 3.3).

Figure 3: Example of guideline advice.

- Notes: notes can be attached to a specific guideline e.g., to record progress with compliance.

Links between guidelines hinge on the identified `Asset` and `Vulnerability` types. For instance, removable storage devices may be secured by password-authenticated encryption, so the user could then consult advice on password quality and usability. Use of an ontology formalises the relations between guidelines from within and across different standards. We focus on guideline relations that identify human-behavioural considerations (e.g. usability of passwords when encrypting removable storage devices).

3.3 Integration of Modelling Tools

CISOs should assess the impact that management decisions will have upon members of an organisation. Modelling tools that assess the usability of security controls can potentially provide further insight into these impacts. This would support decision-making while enabling analysis of various policy scenarios.

Our knowledge base user interface integrates a demonstrative modelling tool that measures password strength and memorability. Much existing research (e.g. (A. Adams, 1997)) has highlighted that password security and memorability are often conflicting goals, so a balance must be found. Here a CISO can enter sample passwords as per their own prospective policies, and be informed of both how secure the password would be and how easy or hard it might be to remember (as determined by a simple demonstrative algorithm). Presenting the tool in this way provides a perspective similar to that of an individual in the organisation. The tool output could be used as evidence for management decisions e.g., whether a specific password format would meet an organisation's usability and security requirements.

The simple password strength/memorability tool demonstrates the potential for using modelling tools to consider human-behavioural factors in security management decision-making. More complex modelling tools with appropriately formalised human-behavioural metrics could be added over time.

4 RELATED WORK

Fenz et al (S. Fenz, 2007) created a security ontology incorporating content from the ISO27001/2 standards. Guidelines are related to organisational security controls, allowing assessment of security policies within the ISO27001/2 framework. Our ontology also incorporates structural components and content from ISO27002, for the purposes of knowledge derivation and expansion.

Lee et al (S. Lee, 2006) describe a process for identifying interdependencies across different standards and deriving security requirements from these standards. Questionnaires are used to align standards and internal security configurations. This work demonstrates adaptation of natural-language standards to internal security infrastructures, by way of information models that identify and relate assets, vulnerabilities etc. We formalise the relationships between guidelines and subject matter within and across information security standards to deepen knowledge and facilitate integration of additional knowledge.

The ENISA Knowledgebase tool (ENISA, 2008) is a directory for managing content from different IT standards. It can be used to decompose standards content and store it in a consistent, systematised format. We break standards down into their structural components, but to the level of objects and procedures that a CISO can consider within their policies.

Commercial tools exist to assist organisations pursuing compliance with external standards (e.g. Cura Compliance (Cura, 2009), Modulo Risk Manager (Modulo, 2009)). These products integrate knowledge of e.g. ISO27002 controls into a compliance process, providing guideline content and additional functionality to relate guidelines with an organisation's information security position (by way of specific organisational assets and processes). Our knowledge base associates external standards with security infrastructure components, allowing further knowledge to be developed and in part tailored to specific organisations.

5 CONCLUSIONS

We have developed a knowledge base structure and associated user interface that expand the informa-

tion security management knowledge available to CISOs, and improve awareness of the relationships between various information security concepts. The work also serves to illustrate how consideration of human-behavioural factors can be incorporated into this knowledge structure. Investigation of the requirements of the interface further informed development of inter-concept connections, and how they are presented to target users.

The decomposition of external standards into individual concepts and relationships, integrated with additional knowledge, provides potential for CISOs to better understand IS management knowledge and so inform their security management decisions further.

There is potential to build upon the work described in this paper, by for instance integrating more complex, specialised modelling tools, and by expanding the range of guidelines in the knowledge base.

ACKNOWLEDGEMENTS

The authors are supported in part by EPSRC grant EP/F066937/1 ("Economics-inspired Instant Trust Mechanisms for the Service Industry") and UK Technology Strategy Board (TSB), grant nr. P0007E ("Trust Economics").

We are grateful for the feedback we received from Robert Coles (Merrill Lynch) and members of the Trust Economics project (Newcastle, 2009). Daria Stepanova was a Visiting Researcher at Newcastle University, visiting from Saint-Petersburg State University, Russia.

REFERENCES

A. Adams, M. A. Sasse, P. L. (1997). Making passwords secure and usable. In *HCI 97: Proceedings of HCI on People and Computers XII*, pages 1–19. Springer-Verlag.

A. Beautement, R. Coles, e. a. (2008). Modelling the human and technological costs and benefits of usb memory stick security. In *Workshop on Economics in Information Security (WEIS)*.

BS (2005). *BS ISO/IEC 27002:2005 - Information Technology - Security Techniques - Code of Practice for Information Security Management*. British Standards Institution.

C. Alberts, A. D. (2004). An introduction to the octave method. http://www.cert.org/octave/methodintro.html. Software Engineering Institute, Carnegie Mellon University, last viewed 12/03/09.

Cura (2009). Cura compliance. Cura Software Solutions, http://www.curarisk.com/pages/content.asp?SectionID=7&SubSectionID=50. last viewed 12/03/09.

Decraene, D. (2009). jowl - semantic javascript library. http://jowl.ontologyonline.org/. last viewed 12/03/09.

ENISA (2008). Knowledgebase: Tool-based security policy composition. European Network and Information Security Agency (ENISA). Version 1.0.

ISACA (2009). *An Introduction to the Business Model for Information Security*. ISACA.

KTN (2007). *Human Vulnerabilities in Security Systems: White Paper*. KTN Human Factors Working Group.

Modulo (2009). Modulo risk manager. http://www.modulo.com/products/modulo-risk-manager-overview.jsp. last viewed 12/03/09.

N. F. Noy, D. L. M. (2000). Ontology development 101: A guide to creating your first ontology. *Stanford KSL Technical Report KSL-01-05*.

Newcastle (2009). Trust economics website. Newcastle University, UK, http://www.trust-economics.org/. last viewed 24/02/09.

R. Coles, J. Griffin, e. a. (2008). Trust economics feasibility study. In *38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008)*, pages A45–A50. IEEE Computer Society.

S. E. Parkin, A. v. M. (2009). An information security ontology incorporating human-behavioral implications. *School of Computing Science, Newcastle University CS-TR No 1139*.

S. Fenz, G. Goluch, e. a. (2007). Information security fortification by ontological mapping of the iso/iec 27001 standard. In *PRDC '07: Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing*, pages 381–388. IEEE Computer Society.

S. Lee, R. Gandhi, e. a. (2006). Building problem domain ontology from security requirements in regulatory documents. In *SESS '06: Proceedings of the 2006 international workshop on Software engineering for secure systems*, pages 43–50. ACM.

Skidmore, P. (2003). *Beyond Measure*. Demos.

Stanford (2009). The protégé ontology editor and knowledge acquisition system. Stanford Center for Biomedical Informatics Research, http://protege.stanford.edu/. last viewed 24/02/09.

UCISA (2005). *UCISA Information Security Toolkit*. Universities and Colleges Information Security Association (UCISA), 3rd edition.

W3C (2004). Owl web ontology language overview. http://www.w3.org/TR/owl-features/. last viewed 24/02/09.