COMPUTING SCIENCE

A Knowledge Base for Justified Information Security Decision-Making

D. Stepanova, S. E. Parkin, A. van Moorsel.

TECHNICAL REPORT SERIES

No. CS-TR-1137 February, 2009

TECHNICAL REPORT SERIES

No. CS-TR-1137 February, 2009

A Knowledge Base for Justified Information Security Decision-Making

D. Stepanova, S. E. Parkin, A. van Moorsel

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.

Printed and published by the University of Newcastle upon Tyne,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne, NE1 7RU, England.

Bibliographical details

STEPANOVA, D., PARKIN, S. E., VAN MOORSEL, A.

A Knowledge Base for Justified Information Security Decision-Making
[By] D. Stepanova, S. E. Parkin, A. van Moorsel.

Newcastle upon Tyne: University of Newcastle upon Tyne: Computing Science, 2009.

(University of Newcastle upon Tyne, Computing Science, Technical Report Series, No. CS-TR-1137)

Added entries

UNIVERSITY OF NEWCASTLE UPON TYNE
Computing Science. Technical Report Series. CS-TR-1137

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.

About the author

Daria (Dasha) Stepanova is a student at St.Petersburg State University, Russia, in the Department of Mathematics and Mechanics. Her specialization is in applied computer studies in sociology. Her research interests also include information security. Daria was a visiting researcher at Newcastle University between September 2008 and March 2009.

Simon Parkin is a Post-Doctorate Research Associate working with Dr. Aad van Moorsel as a member of the Trust Economics project, funded by the Department of Trade & Industry (DTI). Simon completed a BSc Computing Science degree in 2002 and an Advanced MSc degree in "System Design for Internet Applications" (SDIA) in 2003, both at Newcastle University. The latter included an industrial placement at Arjuna Technologies focusing on reliable messaging for Web Services. Between 2003 and 2007 Simon studied a PhD under the supervision of Dr. Graham Morgan. Research subjects covered during this period included E-Commerce, Service Level Agreements (SLAs) and Distributed Virtual Environments (DVEs). Simon also contributed to the EU-funded "Trusted and QoS-Aware Provision of Application Services" (TAPAS) project during this time.

Aad van Moorsel joined the University of Newcastle in 2004. He worked in industry from 1996 until 2003, first as a researcher at Bell Labs/Lucent Technologies in Murray Hill and then as a research manager at Hewlett-Packard Labs in Palo Alto, both in the United States. Aad got his PhD in computer science from Universiteit Twente in The Netherlands (1993) and has a Masters in mathematics from Universiteit Leiden, also in The Netherlands. After finishing his PhD he was a postdoc at the University of Illinois at Urbana-Champaign, Illinois, USA, for two years.

Suggested keywords

INFORMATION SECURITY,
ONTOLOGY,
KNOWLEDGE BASE,
HUMAN-BEHAVIOURAL FACTORS

A KNOWLEDGE BASE FOR JUSTIFIED INFORMATION SECURITY DECISION-MAKING

Daria Stepanova, Simon E. Parkin, Aad van Moorsel
School of Computing Science, Newcastle University, Newcastle-upon-Tyne, UK
dasha_stepanova@list.ru, s.e.parkin@ncl.ac.uk, aad.vanmoorsel@ncl.ac.uk

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 (e.g. ISO 27002 [4]) to manage the security of their assets. Standards such as the ISO27k guideline series offer only management-level recommendations. These recommendations must be adjusted to reflect the specific requirements of individual companies [4]. However, Chief Information Security Officers (CISOs) are often not provided with a complete understanding of the organisation's operational requirements and how IT impacts upon them [5].

Within this paper we relate knowledge extracted from standards to the need for employee behaviour to be considered within information security management. CISOs cannot afford to ignore the human element within the organization [2], and must consider it as part of security management [14]. Organizations must cultivate an awareness of the human-behavioral implications of their internal 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 outside of the workplace, and mandating that all storage devices be encrypted to protect valuable data should a device be lost. Understanding and accommodating the usability needs of employees should be a priority for CISOs [6], as it can help in identifying and managing persistent clashes between security mechanisms and end-users [8].

This paper is focused on structuring knowledge from information security standards so as to provide additional benefits. For this we propose that a knowledge base application be developed to encapsulate facts and processes relating to this specific type of information. We build upon the static content of information security standards by identifying relationships between the different information security concepts within an individual standard. Furthermore, we associate with these concepts additional information relat-

ing to the work behaviours of staff.

We build a knowledge base on top of an information model (or *ontology*), and populate it with management recommendations from multiple information security standards. A knowledge base requires logic to provide a structured means of accessing the information within [13], and so 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. Concluding remarks are found in Section 5.

2 KNOWLEDGE BASE DESIGN

CISOs require more information than they are currently provided with to inform their information security management decisions. We refer here 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 is perceived as external standards for information security management, as these are often used by CISOs to provide a measure of an organisation's security competence.

A second requirement of our work is to present existing and additional (i.e. human-behavioural and usability) criteria to a CISO effectively. This is addressed in the user interface, described in Section 3. Any further knowledge derived from or associated with existing information security management content must be arranged logically, and in such a way that it assists in 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 have been stated elsewhere in [19]):

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

2.2 Scope of the Knowledge Base

The ISO27002 standard was chosen as a context for our work, 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) [15] was chosen as an additional source of information. The UCISA toolkit differs in that its content is specifically targeted towards the needs of educational institutions, and not only by the processes it is intended to manage. As the UCISA standard references and expands upon recommendations in the British Standard BS7799 standard (a predecessor to ISO27002), using these two standards together provides an opportunity to investigate ways of representing knowledge taken from interrelated sources.

The scope of the knowledge base content was restricted to those guidelines that relate to the use of removable data storage devices by employees in the workplace. This allowed us to concentrate and build on previous research findings that have shown the need to consider human-behavioural factors when securing information on removable USB storage devices [17, 20]. Employees may for instance use these devices to carry work that to client premises for presentation, or to transfer work between computers when travelling outside the office.

2.3 Approach to Ontology Development

During the development of the ontology, recommendations for designing ontologies were followed [16]. The structure and content of the ontology was also inspired in part by the work of Fenz et al [10], who developed an information security ontology incorporating ISO27001/2 content for the purposes of risk assessment. This work is further discussed in the Related Work (Section 4).

The ontology was developed using the Ontology Web Language (OWL) [3]. We chose OWL as it is extensible and well-supported. By following ontology design recommendations and coding our ontology and knowledge base content in an ontology language, we provide well-structured, meaningful information security knowledge.

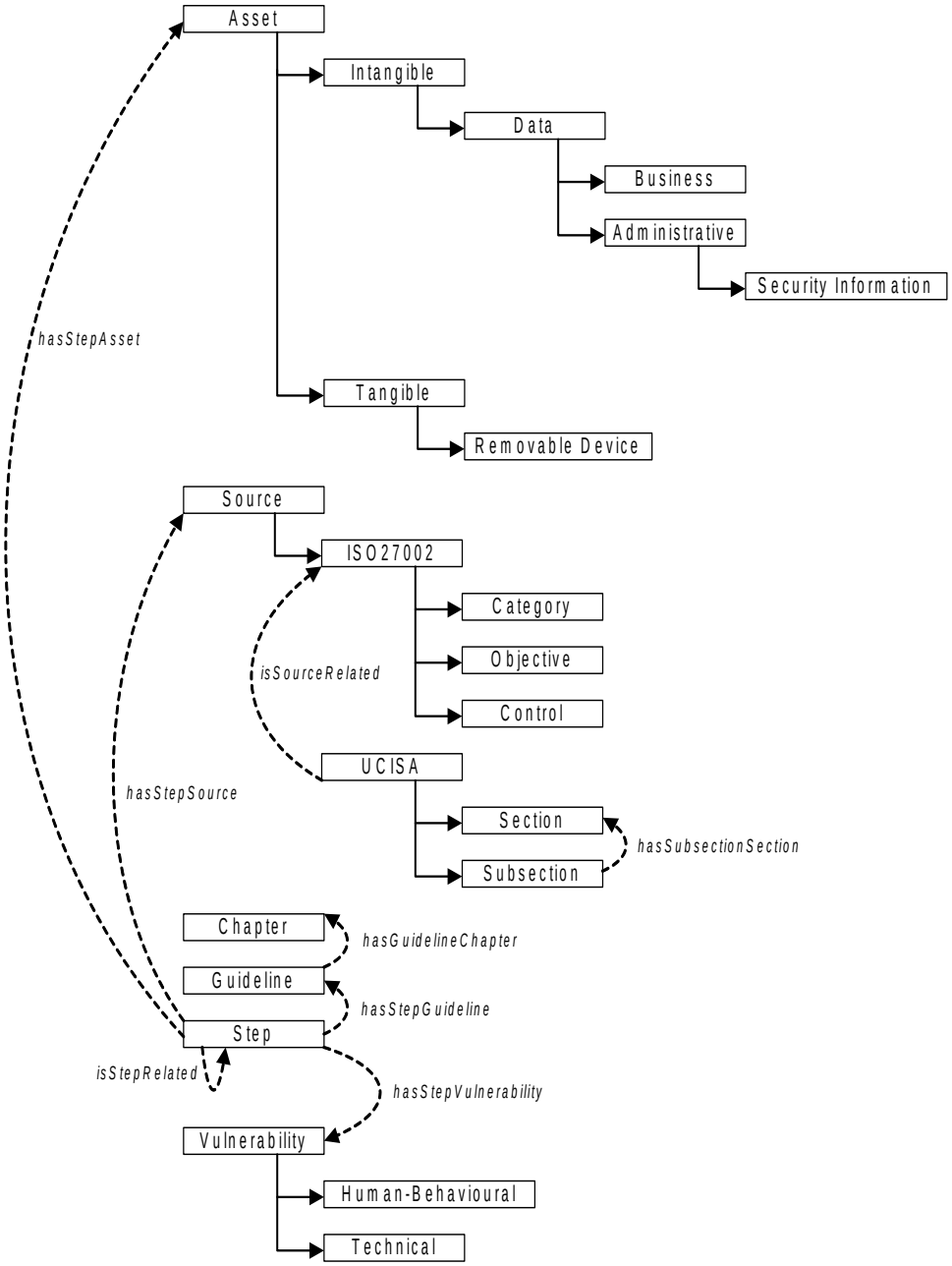

Figure 1: Overview of the ontology.

2.4 Overview of Knowledge Base Components

The content of the ontology is introduced in Figure 1. For brevity the ontology content presented in Figure 1 (primarily asset definitions) is restricted to that 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. Here we focus on a class of tangible `Asset` that we refer to as '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

The `Source` represents the standard from which guidelines are taken. Here we represent two `Sources`, namely ISO27002 and the UCISA Information Security Toolkit. Each standard has corresponding subclasses that describe its structure. The `Source` class allows representation of different sources of information in a single knowledge base, and so it is possible to introduce additional standards in the future (owing to the extensibility of an ontology).

To facilitate integration of different `Source` types into the knowledge base, a single knowledge hierarchy was created to represent information security guidelines. This structure consisted 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 in the workplace was extracted from the standards and arranged according to the aforementioned hierarchy, with a record of the associated `Source`, via the '`hasStepSource`' relation. The '`isStepRelated`' relation serves to formally identify links between (potentially previously non-associated) `Steps`.

Once individual `Guideline` and `Step` instances have been defined, it is possible to identify the `Assets` and `Vulnerability` types that specific recommendations refer to (via the '`hasStepAsset`' and '`hasStepVulnerability`' relations respectively). Each `Asset` then has 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"* (as used in numerous works e.g., [9]). With this we are able to relate human-behavioural vulnerabilities and other additional knowledge to information security standard content in a structured manner.

2.4.3 Vulnerability

In our ontology a `Vulnerability` may be classed as 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 within the organisation). The separation of technical and human factors within an information security standards framework provides CISOs with a formalised perspective on behavioural issues and their relevance to existing IS management concerns.

An example of the connection between an `Asset` and a `Vulnerability` is as follows:

- `Step`: "Security Media Storage"
- `hasStepVulnerability`: "NoProtectionOfUnauthorisedAccess"
- `hasStepAsset`: {"USB", "CD"}

We developed instances of the `Vulnerability` class associated with each guideline and the links that exist between guidelines through decomposition of the ISO27002 standard and UCISA toolkit. Furthermore we consulted experts within a large IT consultancy and reviewed related research documentation. Ideally further ontology content would be developed in a similar manner, through consultation with experienced IS professionals and existing proven research. This approach also proved effective during the work documented in [19], wherein an information security ontology incorporating human-behavioural factors was developed and example content produced to represent the management considerations pertaining to human factors in an organisation's password authentication policy.

3 KNOWLEDGE BASE INTERFACE APPLICATION

We developed a user interface to provide CISOs access to the knowledge base. When creating this interface, we had to consider the usability requirements of CISOs. As such, work on the interface was focused on building a system that bridges the gap between 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 initial interface screen is shown in Figure 2.

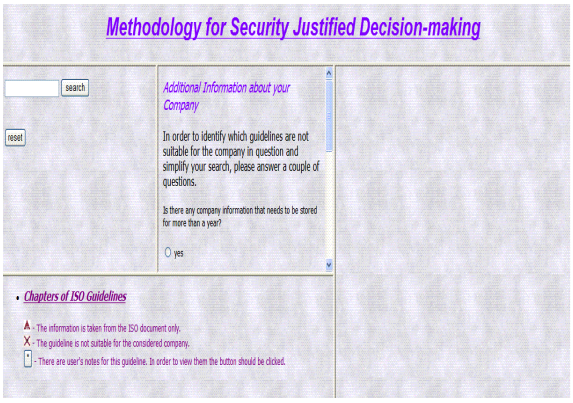

Figure 2: Overview of Knowledge Base user interface application.

In Figure 2 a number of features can be seen:

- Search Window (Top-Left): allows users to search for content that features specific keywords. A CISO may want to locate specific security criteria within a standard, instead of traversing the guidelines in search of it.
- Questionnaire (Middle): a CISO can answer specialised management questions, where the answers are used to refine the guideline set that applies to the organisation. The CISO should not be presented with guidelines that do not apply to their organisation, and this is one means of achieving this.
- Guideline Hierarchy (Bottom): content from information security standards is arranged in a hierarchy to enable simple navigation. In our example content is arranged according to the structure of the ISO27002 standard. Guidelines should adhere to a logical structure and indicate their source, so as to aid in auditing and compliance practices.
- Guideline Information (Right): provides details of specific guideline content, as well as associated `Asset` and `Vulnerability` information. This is the point at which human-behavioural factors are linked to standard content, as it is where the attributes of individual guidelines are presented.

Connections between different guidelines (where they exist) were more readily realised during development of an interface than through ontology design alone. As such the user interface helped to identify possible issues to be addressed for the knowledge base to be effective and useful.

We developed the user interface using HTML, JavaScript and jOWL [18]. 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 most straightforward way to view knowledge base content is to follow the guideline hierarchy to an individual guideline. Each guideline link provides an indication of the source (as shown in Figure 3). CISOs often consolidate and cross-reference recommendations from various sources when developing information security policies, and the aforementioned feature accommodates this.

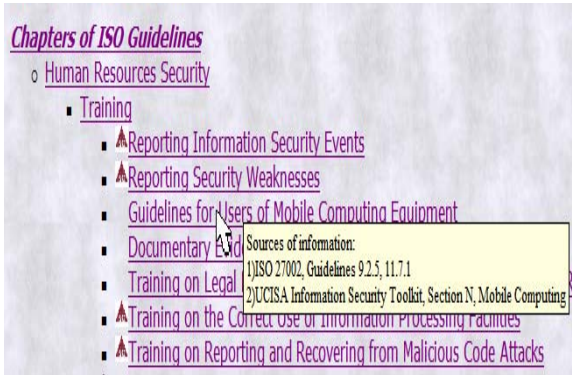

Figure 3: Demonstration of source hints.

Approaching the ontology content via the hierarchy is suitable for users who know which guidelines they wish to view. However it is useful to provide alternative approaches to finding knowledge base content. A logical way to assist the user with their choice is to provide a search engine (as shown in Figure 2). The search engine provides functionality to find mention of specific `Asset` types within the knowledge base. By entering a keyword the user is provided with a list of guideline `Steps` that relate to a named `Asset`. We assume that a user would adhere to the same or similar terminology as found in the related `Sources`. However the knowledge base application utilises synonyms to associate groups of keywords with specific guidelines (e.g., “portable storage device” and “removable media” refer to the same type of `Asset`).

Ontology content can be restricted to serve the needs of a particular organisation by use of the questionnaire shown in Figure 2 (which in this case provides questions relating to removable storage device policy). An applied example would be to ask a CISO if they require data to be stored on removable devices for more than a year at a time (in which case a particular ISO27002 guideline applies). Logic that processes the questionnaire identifies both guidelines that are applicable to the organisation and guidelines that a CISO can ignore.

3.2 Presentation of Guideline Content

When a user has chosen a specific guideline to view, the interface presents the appropriate knowledge base content (as shown in Figure 4).

Figure 4: Example of guideline advice.

Content for each guideline is divided into:

- Content: plain 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 taken from the `Source` or from other sources such as modelling tools (see Section 3.3).
- Notes: a CISO can attach their own notes to a specific guideline (for instance to track their own compliance with the guideline).

Links between guidelines become apparent when the associated `Asset` and `Vulnerability` objects are identified. For instance, an unsecured removable storage device may be protected by password-authenticated encryption processes. The user must then consult advice relating to the quality and usability of passwords. By using an ontology the capability to relate guidelines from within across different information security standards is adequately systematized. Note that we focus on those links between guidelines that identify potential human-behavioural factors (e.g. the usability of passwords when using encrypted removable storage devices).

3.3 Integration of Modelling Tools

CISOs should assess the impact that their management decisions will have upon those individuals that they affect. Modelling tools that assess the usability of security controls can potentially provide further insight into these impacts. This would support decision-making while enabling enterprises to analyse various policy scenarios. As such we chose to accommodate modelling tools in our knowledge base.

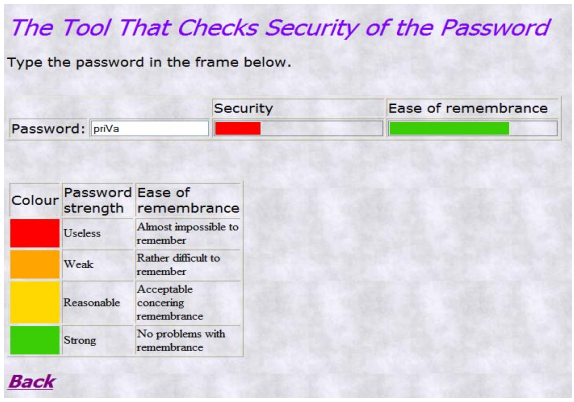

Figure 5: Example password strength/memorability modelling tool.

Our knowledge base user interface contains a simple demonstrative modelling tool for the measurement of password strength and memorability (as shown in Figure 5). Much existing research (e.g. [25]) has highlighted that making passwords secure and ensuring that individuals can remember their own passwords are often conflicting goals, and as such there is a need to find a balance between these two requirements. Here a CISO can enter sample passwords in accordance with their own prospective policies, and be informed not only of how secure the password would be but also how easy or hard it would be to remember. Presenting the tool in this manner provides the CISO with a perspective similar to that of an individual in the organisation. Use of the tool also provides evidence that can be used to justify management decisions (e.g., whether a specific password format would satisfy the organisation's requirements for ease of use and security in practice).

The provision of a simple password strength/memorability test demonstrates the potential for using modelling tools to understand human-behavioural factors within the information security management decision-making process. It is conceivable that more complex modelling tools could be integrated into the knowledge base over time.

4 RELATED WORK

The ROPE methodology [7] and related security ontology [11] provide organisation-wide evaluation of IT security management, focusing on business processes and risk-management. The ontology encapsulates well-known information security concepts such as assets, vulnerabilities, threats and controls.

These form a framework for structuring organisation-specific knowledge, used both for high-level decision-making and as input to risk assessment processes. The security ontology in [11] serves the need of IT managers to communicate qualities of the IT infrastructure so as to better justify their security decisions. We also utilise an ontology to represent the factors that contribute to information security decisions.

A security ontology incorporating guidelines from the ISO27001/2 standards is described in the work of Fenz et al [10]. Here individual guidelines are related to an organisation's security controls, providing a means of assessing internal security policies within the ISO27001/2 framework, and thereby reducing the effort to align standards and policies. Our ontology also incorporates structural components and content from the ISO27002 standard, for the purpose of knowledge derivation and expansion.

Work by Seok-Won Lee et al [12] describes the derivation of security requirements from external standards (including US Department of Defense guidelines). A process is developed for determining interdependencies across different standards. Questionnaires are created to align standards to internal security configurations. This work also demonstrates adaptation of natural-language security standards to internal security infrastructures, including the identification and association of assets, threats, vulnerabilities and controls to guideline requirements, by way of information models. In our work an ontology identifies the relationships between guidelines within and across information security standards to deepen knowledge. We also identify the assets and vulnerabilities that are referred to within specific guidelines, which allows us to integrate additional knowledge in a formalised manner.

Regarding knowledge base applications, the ENISA Knowledgebase tool [24] acts as a directory for managing content from different external IT standards. The tool allows for content from standards to be added and separated into stored sections. In this way it provides a consistent format for storing recommendations and policy advice from different standards. Our work also serves in part to break standards down into structural components, but more so with regards to the objects and procedures to which CISOs must align their policies.

Commercial tools exist to assist organisations actively pursuing compliance with external standards (e.g. Modulo Risk Manager [21], Easy2Comply [22], Cura Compliance [23]). These products integrate knowledge of e.g. ISO27002 controls into a compliance process, providing individual guideline content and additional functionality that a CISO can use to relate guidelines with their organisation's information security position. Tools such as these are primarily driven by the need for organisations to efficiently manage the standards compliance process. As such they provide functionality to correlate specific organisational assets and processes with existing standard content. The structure of our knowledge base can accommodate further knowledge beyond that which is already available in external standards (most notably as relates to the human-behavioural factors involved). It is worth noting however that in practice our tool would then require a suitably qualified expert to derive knowledge of human-behavioural factors in information security management, and record this knowledge appropriately.

5 CONCLUSION

We have developed a knowledge base structure and associated user interface that expand the information 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 advice from 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 covered 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 [1].

Daria Stepanova worked at Newcastle University as a Visiting Researcher, visiting from Saint-Petersburg State University, Russia.

REFERENCES

1. Newcastle University UK, "Trust Economics Website", http://www.trust-economics.org/, last viewed 24/02/09
2. KTN Human Factors Working Group, "Human Vulnerabilities in Security Systems: White Paper", Cyber Security Knowledge Transfer Network (KTN), 2007
3. W3C, "OWL Web Ontology Language Overview", http://www.w3.org/TR/owl-features/, 2004, last viewed 24/02/09
4. British Standards Institution, "BS ISO/IEC 27002:2005 - Information Technology - Security Techniques - Code of Practice for Information Security Management", 2005
5. Christopher Alberts, Audrey Dorofee, "An Introduction to the OCTAVE Method", http://www.cert.org/octave/methodintro.html, Software Engineering Institute, Carnegie Mellon University, last viewed 12/03/09
6. P. Skidmore, "Beyond Measure", Demos, 2003
7. G. Goluch, A. Ekelhart, S. Fenz, S. Jakoubi, S. Tjoa and T. Mueck, "Integration of an Ontological Information Security Concept in Risk Aware Business Process Management", Proceedings of the 41st Hawaii International Conference on System Sciences (HICSS 2008), IEEE Computer Society, pp 377-385, 2008
8. ISACA, "An Introduction to the Business Model for Information Security", ISACA, 2009
9. B. Tsoumas, D. Gritzalis, "Towards an Ontology-based Security Management", Proceedings of the 20th IEEE International Conference on Advanced Information Networking and Applications (AINA '06), 2006
10. S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, and E. Weippl, "Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard", Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing (PRDC2007), IEEE Computer Society, pp 381-388, 2007
11. A. Ekelhart, S. Fenz, M. Klemen, E. Weippl, "Security Ontologies: Improving Quantitative Risk Analysis", pp.156a, 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007
12. S. Lee, R. Gandhi, D. Muthurajan, D. Yavagal, G. Ahn, "Building Problem Domain Ontology from Security Requirements in Regulatory Documents", Proceedings of the 2006 international workshop on Software engineering for secure systems, pp 43-50, 2006
13. J. F. Sowa, "Knowledge Representation: Logical, Philosophical, and Computational Foundations", Brooks Cole Publishing Co., 2000
14. A. Beautement, M. A. Sasse, and M. Wonham. "The Compliance Budget: Managing Security Behaviour in Organisations", In Proc. 2008 Workshop on New Security Paradigms, 2008
15. Universities and Colleges Information Security Association (UCISA), "UCISA Information Security Toolkit", 3rd Edition, UCISA, 2005
16. N. F. Noy & D. L. McGuinness, "Ontology Development 101: A Guide to Creating Your First Ontology", Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, 2001
17. A. Beautement, R. Coles, J. Griffin, B. Monahan, D. Pym, M.A. Sasse, M. Wonham, "Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security", Workshop on Economics in Information Security (WEIS), 2008
18. David Decraene, "jOWL - Semantic Javascript Library", http://jowl.ontologyonline.org/, last viewed 12/03/09
19. S. E. Parkin, A. van Moorsel, "An Information Security Ontology Incorporating Human-Behavioral Implications", CS-TR No 1139, School of Computing Science, Newcastle University, Feb 2009
20. R. Coles, J. Griffin, H. Johnson, B. Monahan, S.E. Parkin, D. Pym, M.A. Sasse, A. van Moorsel, "Trust Economics Feasibility Study", In 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008), IEEE Computer Society, pp A45-A50, 2008
21. Modulo, "Modulo Risk Manager", http://www.modulo.com/products/modulo-risk-manager-overview.jsp, last viewed 12/03/09
22. Easy2Comply, "ISO 27001 Software", http://www.easy2comply.com/ISO27001.htm, last viewed 12/03/09
23. Cura Software Solutions, "Cura Compliance", http://www.curarisk.com/pages/content.asp?SectionID=7&SubSectionID=50, last viewed 12/03/09
24. European Network and Information Security Agency (ENISA), "KNOWLEDGEBASE: Tool-based Security Policy Composition", Version 1.0, ENISA, 2008
25. A. Adams, M. A. Sasse, P. Lunt, "Making Passwords Secure and Usable", Proceedings of HCI on People and Computers XII, pp 1-19, 1997