Newcastle University e-prints

Date deposited: 10th September 2010

Version of file: Published [Newcastle University Computing Science Technical Report]

Peer Review Status: Peer reviewed

Citation for published item:

Mace J C, Parkin SE, van Moorsel A. [*A Collaborative Ontology Development Tool for Information Security Managers*](#). Newcastle upon Tyne:School of Computing Science, University of Newcastle upon Tyne,2010.

Further information on publisher website

Publishers copyright statement:

Use Policy:

The full-text may be used and/or reproduced and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not for profit purposes provided that:

- A full bibliographic reference is made to the original source
- A link is made to the metadata record in Newcastle E-prints
- The full text is not changed in any way.

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Robinson Library, University of Newcastle upon Tyne, Newcastle upon Tyne.

NE1 7RU.

Tel. 0191 222 6000

COMPUTING SCIENCE

A Collaborative Ontology Development Tool for Information Security
Managers

John Mace, Simon Parkin, Aad van Moorsel

TECHNICAL REPORT SERIES

No. CS-TR-1212

July 2010

No. CS-TR-1212

July, 2010

A Collaborative Ontology Development Tool for Information Security Managers

J. C. Mace, S. E. Parkin, A. van Moorsel

Abstract

This paper explores the need for a collaborative development tool to allow information security experts to capture their interrelated knowledge in an ontology. Such a tool would enable organisations to make more informed security policy decisions around shared security issues. However, population of ontologies can be time-consuming and error-prone, and current collaborative ontology editing tools require a familiarity with ontology concepts. We present a Web-oriented tool which simplifies ontology population for information security experts, allowing them to develop ontology content without the need to understand ontology concepts. To understand how organisations manage information security knowledge within policies, we consulted two information security managers in large organisations. The Web-Protégé collaborative ontology editor was then modified to create a tool with an appropriate knowledge ontology structure that meets their requirements. The same information security managers then evaluated the tool, judging it to be accessible and potentially useful in policy decision-making.

Bibliographical details

MACE, J. C., PARKIN, S.E., VAN MOORSEL, A.

A Collaborative Ontology Development Tool for Information Security Managers

[By] J. C. Mace, S. E. Parkin, A. van Moorsel

Newcastle upon Tyne: University of Newcastle upon Tyne: Computing Science, 2010.

(University of Newcastle upon Tyne, Computing Science, Technical Report Series, No. CS-TR-1212)

Added entries

UNIVERSITY OF NEWCASTLE UPON TYNE

Computing Science. Technical Report Series. CS-TR-1212

Abstract

This paper explores the need for a collaborative development tool to allow information security experts to capture their interrelated knowledge in an ontology. Such a tool would enable organisations to make more informed security policy decisions around shared security issues. However, population of ontologies can be time-consuming and error-prone, and current collaborative ontology editing tools require a familiarity with ontology concepts. We present a Web-oriented tool which simplifies ontology population for information security experts, allowing them to develop ontology content without the need to understand ontology concepts. To understand how organisations manage information security knowledge within policies, we consulted two information security managers in large organisations. The Web-Protégé collaborative ontology editor was then modified to create a tool with an appropriate knowledge ontology structure that meets their requirements. The same information security managers then evaluated the tool, judging it to be accessible and potentially useful in policy decision-making.

About the authors

John Mace completed a BSc (Hons) in Computing Science at Newcastle University in 2010 during which time he received a Scott Logic prize for computer excellence for his year two performance. He was also awarded the School of Computing Science prize for best overall performance in year three. John begins a PhD in 2010 under the supervision of Prof. Aad van Moorsel in the area of data security. His research interests include ontologies, cloud computing and tools to support IT security policy making.

Simon Parkin is a Post-Doctorate Research Associate working with Prof. Aad van Moorsel as a member of the Trust Economics project, funded by the UK Technology Strategy Board (TSB). 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. Aad has worked in a variety of areas, from performance modelling to systems management, from web services to cloud computing and on issues of security and trust. In his last position in industry, he was responsible for HP's research in web and grid services, and worked on the software strategy of the company.

His research agenda aims at establishing an intelligent enterprise, with a specific focus on trust, privacy and security. The goal is to provide tools to improve IT decision making, if possible based on objective, quantitative methods, eventually fully automated. This involves mathematical modelling, algorithms and service-oriented software implementations.

Suggested keywords

INFORMATION SECURITY ONTOLOGY
ONTOLOGY EDITOR

A Collaborative Ontology Development Tool for Information Security Managers

John C. Mace

Simon E. Parkin

Aad van Moorsel

School of Computing Science & Centre for Cybercrime and Computer Security (CCCS)
Newcastle University
Newcastle-upon-Tyne, UK
{j.c.mace, s.e.parkin, aad.vanmoorsel}@newcastle.ac.uk

ABSTRACT

This paper explores the need for a collaborative development tool to allow information security experts to capture their interrelated knowledge in an ontology. Such a tool would enable organisations to make more informed security policy decisions around shared security issues. However, population of ontologies can be time-consuming and error-prone, and current collaborative ontology editing tools require a familiarity with ontology concepts. We present a Web-oriented tool which simplifies ontology population for information security experts, allowing them to develop ontology content without the need to understand ontology concepts. To understand how organisations manage information security knowledge within policies, we consulted two information security managers in large organisations. The Web-Protégé collaborative ontology editor was then modified to create a tool with an appropriate knowledge ontology structure that meets their requirements. The same information security managers then evaluated the tool, judging it to be accessible and potentially useful in policy decision-making.

Categories and Subject Descriptors

K.4.3 [Computers and Society]: Organisational Impacts – *computer-supported collaborative work*

General Terms

Human Factors, Management, Security.

Keywords

Information Security Ontology, Ontology Editor.

1. INTRODUCTION

Organisations need to manage the security of their information assets to limit potential abuse or damage within business activities. Information security policies are typically formulated which stipulate at an operational level how these assets should be secured across the entire organisation.

Currently, information security policies are generally informed by a mix of “professional opinion”, staff experience, technology manufacturer advice and external security standards or regulations (e.g. ISO27001 [4]). Sourced IT security knowledge and subjective opinion should be grounded within the organisation’s policies in a structured manner. However there are potentially vast amounts of knowledge pertaining to information security management for organisations available from a variety of global sources and represented by a host of terms and concepts.

This knowledge can be aligned in the form of an ontology. An ontology would serve to standardise the vast array of terms and concepts, and expose the interdependencies between fragments of IT-security knowledge, helping policy makers to make more informed security policy decisions.

Previous work has examined tools to assist CISOs and other IT practitioners in developing information security policies [10][19], and how they might interact with information security knowledge structures such as ontologies [28].

Information security managers and practitioners within different organisations often have to resolve the same or similar IT-security issues (e.g. authentication, remote access, etc.) and explore large amounts of information when doing so. Dissemination of this information throughout the IT security practitioner community in the form of an ontology has not as yet been explored as a specific issue. However, by making collaboration between domain experts an integral part of the knowledge management process, practitioners could share their expertise in an effective manner, deriving increasingly robust solutions to shared security problems.

The Web is a natural platform to host collaborative information security ontology development and facilitate distribution of ontology content. In fact, collaborative ontology creation is typically carried out using Web-oriented ontology editing tools. However, current editing tools tend to be complex and generic in nature. These tools are aimed at those with experience in ontology creation, and not necessarily those domain experts whose knowledge requires capture. It cannot be assumed that Chief Information Security Officers (CISOs) have the appropriate skills in ontology development, as they may be unable to acquire such skills due to a lack of time, inclination, or technical ability. As a result the process of populating an ontology could prove time-consuming and prone to errors during knowledge capture.

Here we consider a collaborative ontology editor tool for use by CISOs. We consider how an ontology should be presented to CISOs to ensure that it is both approachable and useful. We also explore how CISOs might use the features of a collaborative ontology editor to derive knowledge to help improve information security policy decision-making within organisations.

Through consultations with two CISOs within large organizations we build a picture of the process of formulating information security policies within organizations, as well as identifying influential factors that arise within this process. Within these consultations we also explore the potential to share the knowledge

inherent in these policies with the IT-security practitioner community.

Insights from the CISO consultations inform development of a collaborative Web-based ontology development tool intended to serve CISOs or individuals in similar positions in charge of information security policies for organisations. The tool allows direct capture of knowledge – both from disparate sources and created as professional “know-how” – and integration of this knowledge into a centralised ontology-based knowledge repository. The tool limits the need for users to be familiar with ontology construction.

The CISOs consulted earlier within the research participated in a structured evaluation of the ontology editor tool, providing feedback on tool design and functionality. Evaluation sessions also provided the participants with a tangible software tool around which to discuss the preferences they have for a potential knowledge-sharing environment.

The paper is arranged as follows: Section 2 discusses the need for a collaborative ontology effort and current construction approaches. Section 3 discusses capture of requirements for our tool through consultations with real CISOs, and Section 4 details the implementation of the tool. Section 5 presents evaluation findings from follow-up consultations with CISOs, while related work in ontology tools and construction is discussed in Section 6. Concluding remarks are presented in Section 7.

2. BACKGROUND

2.1 Communicating Information Security Policy Decisions

CISOs are the primary decision makers on information security policy within an organisation. The CISO must make decisions on their organisation's security policy that consider not only the security of the organisation's information assets, but also the needs of the business and its employees (be this regulatory expectations or budgetary limitations). By formalising knowledge of various IT-security concerns and exposing their interdependencies, the content of an information security knowledge base would serve to inform and communicate those decisions.

CISOs are part of a wider community of IT-security practitioners and experts tasked with understanding and addressing information security concerns. Teams of information security experts may work within organisations, or may be acting in isolation in different organisations to address similar IT-security concerns.

These experts potentially share information security knowledge within informal or closed groups. The sharing of expertise within relatively small groups exerts limited impact – sharing of this expertise to the wider community exposes it to greater rigour (improving the quality), but also helps global efforts to resolve what are often global information security threats.

2.2 Current Ontology Development

Currently the construction and/or modification of an information security knowledge base or ontology would involve the use of an existing ontology development tool. These typically come in two forms, either graphical or text-based. Graphical tools allow the user to manipulate a graphical representation of knowledge

fragments, while textual editors permit content to be entered manually and arranged in a hierarchical structure.

These different forms of ontology editor place similar demands on the user. The tool user must construct a suitable ontology structure in the tool before knowledge capture can begin. Due to its complex nature this process assumes familiarity with ontology technologies. As such, to create and/or modify an information security ontology, knowledge is required of: ontology creation, including the use of ontology development tools; ontology structure and language; and the ontology content itself.

Most information security domain experts do not have the expertise to create an ontology directly using existing tools as such tools are complex and aimed at ontology experts, and not necessarily those who hold the knowledge that populates those ontologies. As such an information security domain expert may be unable to develop ontology content themselves, and would require either the assistance of an ontology expert or a dedicated ontology editing tool that hides ontology complexity.

Knowledge capture is potentially error-prone and time-consuming, especially if a CISO or similar is relying upon an ontology expert with limited availability who does not fully understand the nuances of the knowledge content and its structure as they enter it into the ontology.

2.3 Collaborative Ontology Development

The creation of an information security ontology is far too large a task for any one individual or small team to carry out effectively. Derivation of knowledge within small teams also limits the applicability and verifiability of knowledge base content.

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 on a robust body of knowledge. For an ontology of information security knowledge to be useful the knowledge it contains must be accepted and trusted by both its providers and its users. Through the involvement of multiple experts, a larger and more applicable knowledge base can be created.

Technology can allow information security domain experts to successfully share in the creation of a knowledge base. The Web is a natural platform for collaboration and knowledge-sharing, by distributing the development process and disseminating the resulting knowledge across the information security community.

3. REQUIREMENTS CAPTURE

A CISO use their knowledge and expertise to compose information security policies, which then inform the IT-security stance of their organisation. We examine the process of information security policy-making through semi-structured discussions with information security managers, through a mixture of surveys and phone interviews. For this we consulted two information security managers: (*CISO1*) has a wealth of experience as a former Chief Information Security Officer (CISO) of a large multi-national financial organisation, and; (*CISO2*) is an information security manager at a leading UK University with previous experience at UK regional councils.

These discussions help us to understand and identify the requirements of policy makers when using information security knowledge. The consultations also build a picture of how policy makers across the community choose to interact with external bodies and other knowledge holders, identifying barriers to the sharing of knowledge and with this the potential uptake of a collaborative ontology editing tool.

3.1 Consultations

The results of our CISO consultations are organised and presented here.

3.1.1 Policy Review Timing

Within the organizations of both *CISO1* and *CISO2* information security policies are reviewed at regular intervals, typically annually. *CISO1* points out that although this is normally the case, reviews may be forced by the emergence of a new threat or with the introduction of a new security technology. With this we may assume that CISOs require access to relevant material for guiding policy decisions regarding new threats and security technologies.

3.1.2 Policy Review Resource Gathering

When reviewing and creating policies, *CISO1* refers to the following sources for guidance:

- Payment Card Industry (PCI) [24]
- ISO27001/27002 security standards [4, 5]
- Information Security Forum (ISF) [15]
- International Information Integrity Institute (I-4) [14]

CISO2 also examines a range of sources for guidance:

- Information Technology Infrastructure Library (ITIL) [16]
- ISO27001/27002 security standards [4, 5]
- The Law Society [26]
- TechRepublic [27]

Although both CISOs work in different sectors, they both refer to the ISO27K family of standards during their work.

Having to refer to a number of independent sources implies the need for this information to be cross-referenced in an appropriate manner.

Within *CISO1*'s organisation information gathered from different sources is entered into a software-based policy management tool, which provides facilities to create information security policy database(s). The tool also allows policy content to be separated according to applicable roles (e.g. system development, human resources, auditors, etc). The tool's databases are by no means complete as they provide only information about standards. There remains a lack of coverage of some other kinds of information, such as industry "best practices" and information for managing human factors within IT security management.

For *CISO2* the majority of gathered information is recorded within the organisation "as-is". Some financial and business information is stored as an information base within an Enterprise Resource Planning (ERP) system [21]. Less than 3% of all the gathered information is formalised and managed within a standardised knowledge repository. This contradicts the need to cross-reference various sources of information.

Where information is stored, it is managed within individual policy categories. This together with *CISO1*'s responses suggest that there are various ways to formalise the arrangement of knowledge content into policies.

3.1.3 Policy Creation

The policy databases in *CISO1*'s organisation are used to create and publish information security policies internally upon the organisation's intranet. During policy creation, the ISO27001 standard acts as an underlying structure. Internal policies are then created according to this structure, and developed through methods including benchmarking, forums and use of informal networks. Internal policies (e.g. software configuration settings, machine build settings) are then quite distinct from external information security standards (e.g. ISO27001).

For *CISO2*, an internal information security policy is created by examining the organisation's trading environment (e.g. business, legal and common practices). *CISO2* uses these practices to facilitate the formation of action plans or strategies to achieve particular IT security-related goals. Policies are defined to help realise these strategies and are put into practice upon approval by senior management. When addressing an information security concern with the forming of a policy, the order of strategy, policy and practice is always followed, suggesting that policies must be seen to be achieving a goal for the organisation.

3.1.4 Policy Reviews

When reviewing information security policy within *CISO1*'s organisation, various parties must be consulted both internally and externally (e.g. human resources, legal counsel, etc). In a regulated industry, regulators must be consulted as they may have their own published guidelines (e.g. Financial Services Authority [11]). Also, the views of both internal and external auditors must be sought to assist in aligning policy initiatives with industry standards.

Once the policy has been decided upon, *CISO1* will talk with "technologists" to determine whether the proposed solution can be integrated into the organisation's applications and systems. The proposed policy is also discussed with "business people" to understand how it would be received within the organisation.

CISO2 also consults both internal and external parties during review of information security policies. These parties include the University Registrar, human resources, internal auditors and external legal counsel specialising in information security. Policies are verified by peers and external advisors (e.g. legal counsel) together with additional checks by JISC certificated legal services [48].

These responses imply a need to communicate knowledge meaningfully to peers and other disciplines.

3.1.5 Policy Justification

For both *CISO1* and *CISO2* it is the case that before a policy is enacted it must be justified to, and supported by, senior management. In *CISO1*'s case policies are discussed in terms of risk and what the effects could be to the organisation without such policies being in place. For *CISO2* debate around policies is framed in terms of impact and reach including legal requirements, financial considerations, personal data protection and intellectual policy. A further consideration noted by *CISO2* (but which is likely applicable for *CISO1*) is the commercial and reputational

risks to the institute without such policies being in place. This implies a need to be able to objectively compare the advantages and disadvantages of particular approaches to IT-security. An ontology would serve to formalise knowledge of security solutions and expose their comparable qualities.

CISO1 noted that situations can arise where objective evidence relating to the impact of potential policy changes is lacking (e.g. effects on employee productivity). Here *CISO1* may rely upon his judgment and expertise to convey the reasons why a particular change in security procedure needs to take place. However *CISO1* notes that there would ideally be evidence at hand to support such an argument, implying a need to identify the objective evidence underpinning expert opinion within security policy decision-making.

3.1.6 Policy Evaluation

Within *CISO1*'s activities, information security policies are typically evaluated for correctness and effectiveness using metrics, but this is not always possible. When assessing technological solutions it is possible to obtain and analyse output from those systems (e.g. the number of e-mails rejected by anti-spam software). However where the behaviour of personnel is involved it is difficult to formulate and measure meaningful metrics. An alternative approach might be to obtain agreements from department managers declaring that security measures will be enacted. These agreements are then reviewed at least annually alongside computer-based employee training and forward-looking agreements, e.g. "I will comply with these measures for the next 12 months". Such "self-assessments" then transfer responsibility for security to individuals.

CISO2 notes yet another approach to evaluating IT security controls, where the security policy evaluation process entails physically observing individuals using human-facing security controls and identifying how those controls are dealt with or how they affect working practices.

Within *CISO2*'s organisation, business processes are also reviewed to see if current security controls are appropriate or whether they can be modified to effect improvement.

That there are various options for managing the assessment of information security controls within organisations, and that their place within business processes must also be accounted for, suggests a need to consider the merits of different methods for evaluating security solutions, and equally how appropriate a particular method might be for assessing a range of policy directives.

3.1.7 Sharing Policy Content

CISO1 states that formal and informal groups of CISOs regularly meet to discuss security issues and share expertise. With this approach, there is potential for organisations to converge on similar solutions, even to a low level (e.g. password composition rules, password reset intervals, etc). Sharing of information security management knowledge then occurs amongst known and trusted parties.

In the academic sector, institutions tend to reach consensus on approaches to information security through regular interaction and sharing of expertise. *CISO2* also corresponds regularly with other non-academic organisations (e.g. local government).

Both *CISO1* and *CISO2* would be hesitant to share policy content that exposes the security stance of their organisation. This suggests that if IT security practitioners across different organisations were to share knowledge, there would need to be a consideration of how to hide the identity of contributors or otherwise maintain knowledge at an abstract level so as not to betray its source (although policies may tend to be framed at a high, operational level as a matter of course).

CISO1 would consider using policy-making knowledge from new and untrusted sources once consensus is established amongst peers. Consensus may potentially be reached through successive edits until the content is agreed (i.e. no-one feels it necessary to edit any further).

For *CISO2*, anonymously supplied information would be considered once it was proven successful elsewhere and recommended from a trusted source. If such proof was unavailable the anonymous content would still be considered if it could be tested in an environment of limited impact and in such a way that it could do no harm to the organisation. This suggests a need for details on how supplied knowledge can be enacted and tested.

3.2 Core Findings

From the discussions with CISOs a number of similarities are apparent, from which assumptions may be drawn regarding the management of knowledge contributing to IT-security policies:

- Information security policies are reviewed at regular intervals or when new security threats or technologies emerge, wherein security procedures are informed by guidance material gathered from a variety of disparate sources.
- Organisations across different sectors may form information security policies, and in turn security controls, according to the same guidelines (e.g. ISO27001/2). This implies that many organisations have similar IT-security requirements which could benefit from collaboration.
- Policy consensus is reached from correspondence and discussion amongst peers alongside the examination of guidelines and regulatory mandates.
- All material that informs policy decision-making (be it guidelines, regulatory mandates, technical documentation, etc.) is recorded "in house" and arranged within distinct, specialised policies, although this is not necessarily conducted in a centralised manner.
- Policy directives are reviewed in consultation with many internal and external parties, notably experts in legal, human resource and technical issues. These parties cannot be assumed to be proficient in the use of ontologies or IT-security.
- There is a need to compare different approaches to resolving information security issues and the evaluation of security controls, and to be able to provide justification for policy directives.

3.3 Tool Requirements

From both the examination of current policy-making approaches and discussions with CISOs, the following requirements of a

collaborative ontology development tool for information security knowledge management have been identified:

1. *Knowledge Capture*: the ontology editor tool must allow capture and organisation of formalised knowledge relating to familiar information security concepts (e.g. assets, vulnerabilities, threats, procedural controls etc). Disparate knowledge fragments may also be interrelated, and users should be able to record these relationships.
2. *Collaboration and Consensus*: an interface should allow collaborative capture of distributed knowledge between disparate parties. There should also be features to allow members of the user community to reach consensus (e.g. by discussing content).
3. *User Guidance*: users must be guided through all aspects of ontology development and exploration using “non-ontological” terms and concepts. There should also be appropriate mechanisms to minimise errors.
4. *Knowledge as Evidence*: it may be necessary to present ontology content to other stakeholders (such as senior management) whenever policy-related knowledge is used to justify the management of risks to the organisation.
5. *User Anonymity*: users must be able to preserve an appropriate level of anonymity. Users should not be expected to divulge specific organisation security practices.

4. IMPLEMENTATION

In light of the tool requirements we propose the creation of a collaborative security ontology editing tool to allow members of the CISO community to capture and share their knowledge first-hand. Importantly this tool should remove the need to understand ontology construction techniques. The tool must allow these experts to construct and/or modify, share and analyse a security ontology at an abstract level without the need to familiarise themselves with ontology technologies.

The open-source ontology editor Web-Protégé [1] forms the foundation of the tool. Web-Protégé is a Web-accessible collaborative ontology editor built with a number of collaborative features that can be tailored to meet our requirements.

4.1 Overview of Tool Components

Figure 1. Overview of ontology development tool's components

An overview of the components of the collaborative information security ontology editing tool is shown in Figure 1. The tool is composed of the client-side *Tool Interface* and the *Tool Server*.

4.1.1 Tool Interface

A browser-accessible Web application through which ontology content is viewed and manipulated. The tool interface and its functionality are described in further detail in Section 4.2.

4.1.2 Tool Server

The tool is stored as a Web application archive file on a centralized Web application server. The server provides remote access to the latest version of the tool.

A *War file* contains both the tool system files and the ontology files. Having all the necessary files in a single archive allows for simple server deployment. *Tool system files* within the *War file* hold the tool's compiled source code and supporting images and html pages. All of the tool's current ontology files are stored in the *Projects directory*. The project directory also contains the tool's *Metaproject* ontology file, which describes access conditions for the tool's ontologies.

4.2 Foundation Ontology

Figure 2. Overview of the information security and human factors ontology.

To satisfy the need for formalised knowledge and the capability to relate fragments of knowledge, a suitable ontology must be provided. An information security ontology should define the most important security issues and concepts and the relationships between them. For these purposes the tool uses a modified version of the ontology developed by Parkin, van Moorsel and Coles [23] (Figure 2). This ontology is similar to others that represent information security knowledge (e.g. [10]), but informs policy decision-making further by representing the relationship between human-behavioural factors and other concerns within information security management (e.g. provision of password authentication policies that are both suitably secure and realistic for employees).

The ontology represents the security and usability weaknesses of an *Asset* that may promote or inhibit certain employee

behaviours in relation to security mechanisms or processes. This is embodied in the *Vulnerability* concept.

A *Vulnerability* may be intentionally or accidentally ‘exploitedBy’ a *Threat*, which then renders the *Asset* potentially insecure. A *Threat* represents activities that directly affect security mechanisms or elements of security-facing human behaviour. For each *Threat* the Behavioural Foundation serves to classify behaviours and indicate the concerns that they raise within an organisation (e.g., a person’s memory capabilities or attitude towards security).

A *Vulnerability* may be ‘mitigatedBy’ a *Behaviour Control*, which is considered to be a procedural control enacted by a CISO to manage the interactions between humans and the organisation’s security mechanisms. A *Behaviour Control* ‘managesRiskOf’ a specific *Threat* using a risk management approach indicated by the associated *Control Type*.

Representing information of this nature in this formalised manner clarifies knowledge, and by exposing the relationships between concepts an element of accountability can be provided to support the communication of policy decisions to peers and organisation stakeholders. The tool presented here facilitates use of the ontology in this way.

4.3 Tool Interface

The Tool Interface allows CISOs to access ontology content in a manner that abstracts away details of ontology construction. Users are then free to view, add, modify or relate fragments of IT-security knowledge to help them:

- View information security management knowledge and the interdependencies between knowledge fragments.
- Record (and share) knowledge of information security concerns (through use of editing controls).
- Collaboratively refine the knowledge stored within the underlying ontology, using the tool’s collaboration features.

4.3.1 Accessing the Tool

Users are initially presented with a screen offering a list of available ontologies. For demonstration purposes distinct ontologies are provided so as to mirror an organisation’s policies (e.g. USB stick policy, password policy, etc.). These ontologies employ the structure described in section 2.2, and can potentially be pre-populated with knowledge content that can be viewed and/or extended with user-supplied knowledge.

The main user interface consists of a number of tabbed pages providing users with ontology content, ontology editing controls, and features to advise users in how to interact with the tool. Only authorised users can access editing controls and make changes to the ontology, by providing a registered user ID and password.

4.3.2 Guidance for Users

A “Welcome” page (Figure 3) provides an overview of the tool, its functionality, and the base ontology structure, so as to familiarise new users and act as a reference for returning users. The *Class* and *Property* tab pages provide the user with descriptions of the ontology’s structural components and how they interact with each other.

Figure 3: Screenshot of tool’s ‘Welcome’ page

4.3.3 Editing Ontology Content

Figure 4: Screenshot of a ‘Content’ page

The *Content* pages (Figure 4) allow a user to view and edit ontology content. Any modifications made to an ontology are immediately visible to all those users currently accessing the tool, thereby making it useful in situations that require newly-available knowledge (e.g. when a new threat or technology emerges).

Four separate *Content* pages cover the main classes of the information security ontology structure; *Assets*, *Vulnerabilities*, *Threats* and *Behaviour Controls*. This allows a user to access ontology content from a range of perspectives rather than be restricted to a particular starting point.

Each of the *Content* pages contains a portlet listing the individual fragments of knowledge associated with the particular class. Selecting one of these individuals will display the properties associated with it (e.g. the *Vulnerabilities* of a selected *Asset*). A combination of editing controls and dialog boxes allow a user to add a new class individual or change the text of an existing entry. Warning mechanisms limit the potential for user error and ontology inconsistency (e.g. to prevent addition of an individual with the same text as an existing entry).

Users can also “connect” fragments of knowledge according to the relationships defined in the ontology structure. The tool

restricts the user's choice of property connections accordingly by way of restrictive controls, for example a user may only connect an individual *Vulnerability* to a *Threat* or *Behaviour Control* via the 'exploitedBy' and 'mitigatedBy' properties respectively.

Each Content page has an information portal providing an overview of that page's content and relevant instructions on how ontology content may be extended and/or edited.

4.3.4 Collaborative Features

A *Notes* portal (Figure 5) enables users to annotate, discuss and reach consensus on ontology content by "posting" messages, akin to a bulletin-board system. Posted messages are linked with specific content and are visible to all users when that content is selected. Authorised users may post new messages or reply to pre-existing messages via an e-mail style dialog box.

Figure 5: Screenshot of 'Notes' portal

5. USER EVALUATION

An assessment of the tool's effectiveness in supporting the capture and sharing of information security knowledge by CISOs (or similar) would require a prolonged study that is beyond the scope of this paper.

For the purposes of this paper we conduct an evaluation of the functionality and usability of the tool by presenting it to the CISOs consulted during the Requirements Capture stage (see Section 3).

During evaluation the tool was demonstrated according to a structured demonstration plan, and the chance offered to participants to practice using the tool first-hand. This was immediately followed by a series of structured questions that serve to relate each participant's impression of the tool to the tool's requirements (as defined in Section 3.3).

As well as evaluating the requirements that were defined for the tool, the evaluation sessions provided the opportunity to centre discussion of collaboration and knowledge-sharing around a tangible tool, eliciting comments about how the tool may be practically applied (along with any issues that have the potential to limit application of this, or a similar, tool).

Each complete session was voice-recorded to allow us to capture feedback from the participants throughout the evaluation process.

5.1 Summary

The tool satisfies the requirements outlined in Section 3.3. A summary of other key points that emerged from the evaluation sessions is as follows:

- The tool is approachable and easy to use.
- Care must be taken if dividing the underlying ontology according to distinct policies, as this may cause confusion.

- Concentrating the tool towards particular sector- or organisation-specific concerns may distort content that is essentially shared. Solutions include providing facilities to "tag" relevant content.
- Content duplication could cause problems that might only be resolved through concerted efforts by community members.
- Collaborative features can help users to reach consensus, but must provide proper incentives to maintain a collective community effort.
- Users would be able to preserve their anonymity with the tool, but would need reassurances that it does not disclose the organisation's security posture.
- The tool can support communication of policy decisions to stakeholders, however to fully exploit this capability ontology content would need to include or be enriched with relevant sector- or organisation-specific content.

5.2 Evaluation Sessions

5.2.1 Knowledge Capture

Overall, the tool was considered as being approachable and easy to navigate, with a clear ontology structure, thereby making progress towards accommodating the needs of target users. *CISO2* stated that "regular IT security folk will be able to dig into [the tool] and use it". The tool's user interface was not thought to be confusing but instead very clean, with a "nice flow round the screen" (*CISO1*). *CISO2* regarded the ontology structure, covering *Assets*, *Vulnerabilities*, *Procedural Threats* and *Behaviour Controls*, seemed "very obvious".

The notion of separating ontology content, thus making the ontology more manageable, was described by *CISO2* as a very complex area, but that "splitting the content into policies makes sense". However *CISO1* argued that it might be preferable to "slice and dice the content whatever way the user chooses", and that individual users might potentially not recognise policy content that they would otherwise think is relevant to them if it is not appropriately labelled. For example, a security manager might regard "identification and authentication" as separate technologies, whereas another manager would regard the same content as "sign-on" policy. This problem of potentially unexpected terminology "makes it less accessible in some ways".

With the capturing of content, the tool was described by *CISO2* as generic and "open enough to do just about anything in information security", qualified with examples of issues within networking management, such as firewalls, denial of service attacks, and routing. The tool can potentially capture knowledge of sophisticated information security issues which can "become horribly complex but you could end up with areas of specialisation".

CISO2 suggested that ontology content could be 'tuned' according to the user's business sector, for example banking. However, each sector tends to have slight differences in information security needs, and so any content considered irrelevant to that sector would be omitted from the user interface. However, it would depend on "who takes up the idea [of the tool] first, so making it a while before tailoring content becomes an issue". Alternatively, *CISO1* suggested that one incentive to use the tool "would be if you could tag items to make it specific to your organisation and then ... download an extract or have a

version of it which is for your own organisation, so that you can ignore stuff which isn't relevant to you". CISO2 made a similar comment that keeps content within the tool, suggesting that when users are creating an account they should declare their business sector so that the tool may tailor content to that sector once the user is logged in.

The mechanism which detects whether content is already added was described by CISO2 as good, but the recognition of similar content is not addressed. Not having this feature was considered "a bad thing", as there was potential for multiple entries to describe the same concept. CISO1 built upon this issue, speculating that duplicates might go beyond spelling (e.g. "pwd" instead of "password") to similar terms that use natural alternatives (e.g. "user ID ... logon ID ... username ... credential").

Currently the tool relies on users to use the collaborative features to inform others when similar content is already expressed in the ontology. CISO2 stated that this notion "would probably work" as the "community will police itself to a certain extent but if too much policing is needed [the community] will get tired of it". CISO1 echoed this – "what's the incentive ... to edit somebody else's content?", "just because it's easy doesn't give me a carrot to want to do it" – and suggested a solution of employing an administrator to "collapse" duplicates (which potentially defeats the purpose of the tool).

5.2.2 Collaboration and Consensus

CISO2 considered the collaborative features very useful in discussing knowledge with peers or other stakeholders within an organisation. The ability to add notes to content was described as "a nice feature" that "added richness to the tool". When discussing a threat a user could 'post' a message asking "how real is this threat?" while the reply could be "we've actually had a breach on this". The attachment of messages to specific content made "perfect sense".

Regarding the collaborative features, CISO1 said that "it's a time-save thing" so that users are "not having to reinvent the wheel" at each organisation. However CISO1 also speculated that "within the organisation, that time-saving doesn't mean anything" unless it is with auditors.

For CISO2 the idea suggested of providing additional mechanisms for reaching consensus, such as a voting or rating system, could be seen as being useful. This would be akin to "Ebay where the voting on how good a vendor and supplier are is a big deal". Such a mechanism promotes sensible levels of discussion while ensuring that content stays appropriate: "You end up with the community vetting itself which is what you want to do". CISO1 speculated however that users might inevitably just "grab" meaningful content, returning to the issue of how to "incentivise people to comment and use" the tool.

According to CISO2 encouragement for users to record and share their knowledge may be brought about by stressing, "this is your community and your tool to help you. The richer you make it the more powerful it becomes". A suggestion was to implement a system where users are asked to review recently added content, perhaps through an e-mail style inbox that highlights content added since their last login.

It appears from the evaluation responses that the need for users to be able to discuss content and be aided in reaching consensus has

been achieved, at least in part, via the notes feature. Realistic suggestions for further mechanisms include a voting/rating system enhancement to facilitate content selection.

5.2.3 User Anonymity

CISO2 noted that the user interface did not raise any privacy or security concerns as the user's organisation is not being identified during content entry. The notion of anonymity is achieved by users logging into the tool through a 'username' alias. CISO2 suggested the tool should "stress the fact that content can be entered anonymously and content cannot be traced back to an organisation". CISO1 echoed this concern: "the only drawback would be the level of comfort ... over the ... secrecy around the specificity to my organisation ... how would I know that other people can't see that?".

The mechanism for users to create an account, once implemented, must "vet people and make sure not just anyone can gain access" (CISO2).

The suggestions by both CISOs for personalising ontology content bring with them similar issues of guaranteeing that personal identifiers remain protected.

It appears from the evaluation responses that the need for users to submit information while not divulging specific organisation security practices can be achieved within the tool, although there are understandably many concerns surrounding the issue of user anonymity.

5.2.4 User Guidance

CISO1 thought that the tool was helped by a "very nice layout" that was "not confusing". According to CISO2 the user interface was not thought to be confusing but seemed "fairly simplistic" suggesting an appropriate level of detail for 'non-ontology' experts building an ontology of information security knowledge.

CISO1 suggested that users "might ... want to follow something all the way through" to "produce another view", such that the interface changes dynamically depending on selected content (e.g. moving automatically to another screen).

CISO2 noted that "two or three different learning styles are catered for" by the help features, for example the 'Welcome' screen provides an overview of the ontology structure in both graphical and textual form. "Some people will read the prose while others will use the picture. For me the [diagram of] the knowledge base structure was very useful".

The tool has the capacity to guide users through aspects of ontology development and exploration, using a variety of help features.

5.2.5 Knowledge as Evidence

In relation to the potential for ontology content to be used in communicating and supporting policy decisions, CISO1 speculated that "you'd want to use this ... because it takes you through a structured way of doing a risk assessment ... but the only way that you'd want to do it is if you can make it specific to your organisation", reiterating the idea of "tagging" organisation-specific content. CISO2 similarly "would use [the tool] and happily add content but would need to see the outputs" before using it within their organization ("Would it allow me to make a business case? ... Something that would support that would be really useful") before going on to speculate that if the tool was

being used to assess threats etc. in a particular business sector then *"it would be good enough as it is"*. CISO1 echoes similar thoughts: *"what makes it information is the specificity for your situation"*.

CISO2 noted that an information security manager *"cannot simply say we need to implement this because we are insecure"*. The manager must be able to present a business case to justify changes in IT security policy to senior management from a range of possible solutions, and *"the tool allows you to do that"*. The business case will state *"we can do this, this and this to get us there and then do calculations to work out the costs"*. A scenario could be imagined where departmental managers (e.g. finance or IT helpdesk) are consulted when making security policies and who use the tool's content to help work out costs: *"at the very least [the tool] helps to identify stakeholders to communicate with"*.

5.2.6 Further Comments

Some extensions to the tool's underlying ontology structure were suggested during the evaluation sessions. Such extensions could include – according to CISO1 –, details of *"technical controls"* and their threat management approach (e.g. *"detective"*, *"defending"*). CISO2 suggested that policy implementation costs, methods of policy enforcement and measurements of policy success would be useful (*"Cost is a big deal. Quantifying cost, cost of implementation, cost of risk etc. [is important] but it will be hard to categorise the financial [costs]"*).

6. RELATED WORK

A number of works have been conducted to develop information security ontologies, complimented by an array of collaborative tools resulting from a growing interest in the Semantic Web.

Donner [8] discusses the need for an ontology to describe the most important security concepts and their interrelationships. Such an ontology is needed to provide explicit meaning to the current, vaguely defined terminology and allow clear and effective communication between colleagues and their clients. Vulnerabilities to IT security systems and information would be classified allowing the detection of possible threats and their countermeasures. The discussion ends with the proposal that the ontology should be developed in a collaborative manner.

Formalising information security knowledge for the purpose of auditing and aiding with policy making has been shown to be viable through a number of studies (e.g. [9], [10], [13], [23]). Fenz et al [10] integrate the ISO/IEC 27001 guidelines [4] with their own security ontology which considers the physical aspects of information security. Organisations can use the ontology and accompanying the "OntoWorks" toolset to automatically review and examine IT security policies for ISO 27001 compliance and/or certification.

The ontology by Parkin, van Moorsel and Coles [23] that is used here has also been used by Mace, Parkin and van Moorsel [19] as the foundation for an existing information security ontology editing tool tailored for domain experts. Experts are able to intuitively capture and formalise their knowledge while the ontology construction itself is abstracted away. This tool concentrates on single-site deployment, and so is not Web-oriented and lacks collaborative features.

Collaborative ontology development permits users to access and edit the same ontology from distributed locations. The main features identified for successful collaborative ontology development are discussed in [3] and [20]. 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.

A host of generic Web-oriented collaborative ontology tools are available aiming themselves at users with varying degrees of experience in ontology construction and offering various techniques in knowledge capture and representation, e.g. [18, 22, 25]. A survey of selected tools is carried out in [6]. OntoWiki [2] serves to decrease the entrance barrier for domain experts to capture their knowledge and collaboratively develop ontologies. OntoWiki combines existing Wiki systems and Semantic Web knowledge representation models. The simplification of knowledge acquisition and presentation is brought about by considering ontologies as "information maps". Each node or concept in the map is represented visually in its own page and allows intuitive viewing, editing and linking to other concepts and resources. COE (Collaborative Ontology Environment) [12] builds on the rapid construction techniques of CmapTools [7] and its concept mapping system to represent domain knowledge. An ontology viewing area and collaborative editing environment are combined within COE which then displays ontologies as concept maps. The tool converts these human readable maps into a machine readable ontology language. Concepts from other Web-based ontologies may be incorporated into an ontology, allowing the capture of knowledge from a wide variety of sources.

These tools are aimed towards the domain expert and primarily attempt to make collaborative ontology development and knowledge sharing more accessible. They do however remain relatively complex, are generic in nature and require a substantial amount of initial training and configuration before knowledge owners can begin the knowledge capture process.

7. CONCLUSION

We have shown that there is a need for a collaborative ontology development tool to allow information security experts (namely CISOs or similar) to capture and share their knowledge.

Here we have taken the needs of CISOs into consideration through CISO consultations, and developed a collaborative, Web-hosted ontology editor tool as a deployable application, allowing community users to record and share their knowledge within the structure of a pre-defined information security ontology.

The tool has the potential to improve the IT policy making process by providing the information security management community with a single, shared, comprehensive reference for information security knowledge.

The tool's current implementation has been evaluated by two CISOs from varying backgrounds, meeting with general praise for both its appearance and functionality. We look to address concerns raised about the control and quality of content through enhancement of the tool's collaborative features. This may include provision of a voting system or content-rating scheme.

Future work also hopes to consider the suggestions from participating CISOs for extensions to the underlying ontology

structure, but also the issue raised of potential incentives for motivating members of the information security management community to contribute to a tool such as has been described here.

8. ACKNOWLEDGEMENTS

The authors are supported in part by UK Technology Strategy Board (TSB), grant nr. P0007E ("Trust Economics") and HP Labs Innovation Research Program, award ID 2009-1052-1-A ("Prediction and Provenance for Multi-Objective Information Security Management").

9. REFERENCES

- [1] Tudorache, T., Vendetti, J. And Noy, N. F. 2008. Web-Protege: A lightweight OWL ontology Editor for the Web. In *Proceedings of the 5th OWL Experiences and Directions Workshop*, (Karlsruhe, Germany, 2008), CEUR-WS.
- [2] Auer, S., Dietzold, S. and Riechert, T. OntoWiki – A Tool for Social, Semantic Collaboration. In *Proceedings of the 5th International Semantic Web Conference*, (Athens, USA, 2006), Springer, 736-749.
- [3] Bai, F. and El Jerroudi, Z. Interactive and Collaborative Ontology Development. In *Proceedings of Mensch & Computing 2008 and DeLFI Cognitive Design 2008*, (Berlin, 2008), Logos Verlag, 174-179.
- [4] British Standards Institution' BS ISO/IEC 27001:2005 – Information Technology – Security Techniques – Information Security Management Systems – Requirements, 2005.
- [5] British Standards Institution, BS ISO/IEC 27002:2005 – Information Technology – Security Techniques – Code of Practice for Information Security Management, 2005.
- [6] Buraga, S. B. Cojocaru, L. and Nichifor, O. C. 2006. *Survey on Web Ontology Editing Tools*. Technical Report. University of Iasi, Romania.
- [7] Canas, J., Hill, G., Carff, R., Suri, N., Lott, J., Gomez, G., Eskridge, T. C., Arroyo, M. And Carvajal, R. CmapTools: A Knowledge Modeling and Sharing Environment. in *Proceedings of the 1st International Conference on Concept Mapping*, (Pamplona, Spain, 2004), IHMC, 125-133.
- [8] Donner, M. Towards a Security Ontology, *IEEE Security and Privacy*, 1(3). 6-7.
- [9] Ekelhart, A and Fenz, S. Formalizing Information Security Knowledge. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, (Sydney, 2009), ACM, 183-194.
- [10] Fenz, S., Goluch, G., Ekelhart, A., Riedl, B and Weippl, E. Information Security Fortification by Ontological Mapping of the ISO/IEC270001 Standard. In *Proceedings of the 13th IEEE Pacific Rim International Symposium on Dependable Computing*, (Melbourne, 2007), Springer, 381-388.
- [11] Financial Services Authority (FSA). Retrieved 10 November, 2009, from the Financial Services Authority: <http://www.fsa.gov.uk/>.
- [12] Hayes, P., Eskridge, T. C., Reichherzer, T., Saavedra, R., Mehrotra, M. and Bobrovnikoff, D. Collaborative Knowledge Capture in Ontologies. In *Proceedings of the 3rd International Conference on Knowledge Capture*, (Banff, Canada, 2005), ACM, 99-106.
- [13] Herzog, A., Shahmehri, N. and Duma, C. An Ontology of Information Security, *International Journal of Information Security and Privacy*, 1(4), 1-23.
- [14] I-4. Retrieved 27 January, 2010, from the International Information Integrity Institute: <https://i4online.com/>.
- [15] Information Security Forum Ltd.: Welcome to ISF. Retrieved 27 January, 2010, from Information Security Forum Ltd.: <https://www.securityforum.org/>.
- [16] Information Technology Infrastructure Library (ITIL). Retrieved 24 March, 2010, from APM Group Ltd.: <http://www.itil-officialsite.com/home/home.asp>.
- [17] Joint Information Systems Committee (JISC). Retrieved 24 March, 2010, from Joint Information Systems Committee: <http://www.jisc.ac.uk/>.
- [18] Knoodl: Welcome to Knoodl. Retrieved November 30, 2009, from Revelytix, Inc.: <http://knoodl.com/ui/home.html>.
- [19] Stepanova, D., Parkin, S.E., van Moorsel, A., A Knowledge Base for Justified Information Security Decision-Making. In *Proceedings of the 4th International Conference on Software and Data Technologies (ICSOFT)*, 2009.
- [20] Noy, N. 2007. What Users Want: Collaborative Development of Ontologies. Technical Report. Stanford University, USA.
- [21] O'Leary, D. E. Enterprise Resources Planning Systems: Systems, Life Cycle, Electronic Commerce and Risk, Cambridge University Press, Cambridge, 2000.
- [22] Ontolingua. Retrieved November 30, 2009, from Knowledge Systems, AI Laboratory, Stanford University: <http://www.ksl.stanford.edu/software/ontolingua/>.
- [23] Parkin, S.E., van Moorsel, A. and Coles, R. An Information Security Ontology Incorporating Human-Behavioural Implications. In *Proceedings of the 2nd International Conference on Security of Information and Networks*, (Cyprus, 2009), ACM, 46-55.
- [24] PCI Security Standards Council. Retrieved 27 January, 2010, from the PCI Security Standards Council: <https://www.pcisecuritystandards.org/>.
- [25] Sure, Y., Angele, J. And Staab S. OntoEdit: Multifaceted Inferencing for Ontology Engineering, *Journal on Data Semantics*, 1(1). 128-152.
- [26] The Law Society. Retrieved 24 March, 2010, from The Law Society: <http://www.lawsociety.org.uk/home.law>.
- [27] TechRepublic. Retrived 24 March, 2010, from CBS Interactive Inc.: <http://techrepublic.com.com/>.
- [28] Mace, J., Parkin, S. E., van Moorsel, A., Ontology Editing Tool for Information Security and Human Factors Experts. *CS-TR N° 1172, School of Computing Science*, Newcastle University, Sep 2009