COMPUTING SCIENCE

An Information Security Ontology Incorporating Human-Behavioral Implications

S. E. Parkin, A. van Moorsel.

TECHNICAL REPORT SERIES

No. CS-TR-1139 February, 2009

TECHNICAL REPORT SERIES

No. CS-TR-1139 February, 2009

An Information Security Ontology Incorporating Human-Behavioral Implications

S. E. Parkin, A. van Moorsel.

Abstract

In this paper we explore the need to understand the human-behavioral factors within an organization's information security management processes. We frame this investigation around development of an information security ontology. This ontology is intended for use within organizations that aim not only to maintain compliance with external standards, but also to consider and adjust the attitude towards security as exhibited by those within the organization. We provide an ontology that combines information security standards (in this case ISO27002) and representation of the human-behavioral implications of information security management decisions.
Our ontology explicitly represents the human-behavioral concerns attached to specific security processes and policy decisions. As such it encourages consideration of the security behavior of individuals towards technical security controls. We demonstrate use of our ontology with an applied example concerning management of an organization's password policy. This example illustrates how password configuration may be perceived by individuals within the organization, and how this perception alters their behavior and consequently the attitude to information security in the workplace.

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

Bibliographical details

PARKIN, S. E., VANMOORSEL, A.

An Information Security Ontology Incorporating Human-Behavioral Implications
[By] 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-1139)

Added entries

UNIVERSITY OF NEWCASTLE UPON TYNE
Computing Science. Technical Report Series. CS-TR-1139

Abstract

In this paper we explore the need to understand the human-behavioral factors within an organization's information security management processes. We frame this investigation around development of an information security ontology. This ontology is intended for use within organizations that aim not only to maintain compliance with external standards, but also to consider and adjust the attitude towards security as exhibited by those within the organization. We provide an ontology that combines information security standards (in this case ISO27002) and representation of the human-behavioral implications of information security management decisions.
Our ontology explicitly represents the human-behavioral concerns attached to specific security processes and policy decisions. As such it encourages consideration of the security behavior of individuals towards technical security controls.
We demonstrate use of our ontology with an applied example concerning management of an organization's password policy. This example illustrates how password configuration may be perceived by individuals within the organization, and how this perception alters their behavior and consequently the attitude to information security in the workplace.

About the author

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.

Aad has worked in a variety of areas, from performance modelling to systems management, web services and grid computing. 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.

Suggested keywords

INFORMATION SECURITY ONTOLOGY,
HUMAN BEHAVIORAL IMPLICATIONS,
PASSWORD POLICY

An Information Security Ontology Incorporating Human-Behavioral Implications

Simon E. Parkin*
School of Computing Science
Newcastle University
Claremont Tower
NE1 7RU
Newcastle-upon-Tyne, UK
s.e.parkin@newcastle.ac.uk

Aad van Moorsel
School of Computing Science
Newcastle University
Claremont Tower
NE1 7RU
Newcastle-upon-Tyne, UK
aad.vanmoorsel@newcastle.ac.uk

ABSTRACT

In this paper we explore the need to understand the human-behavioral factors within an organization's information security management processes. We frame this investigation around development of an information security ontology. This ontology is intended for use within organizations that aim not only to maintain compliance with external standards, but also to consider and adjust the attitude towards security as exhibited by those within the organization. We provide an ontology that combines information security standards (in this case ISO27002) and representation of the human-behavioral implications of information security management decisions.

Our ontology explicitly represents the human-behavioral concerns attached to specific security processes and policy decisions. As such it encourages consideration of the *security behavior* of individuals towards technical security controls.

We demonstrate use of our ontology with an applied example concerning management of an organization's password policy. This example illustrates how password configuration may be perceived by individuals within the organization, and how this perception alters their behavior and consequently the attitude to information security in the workplace.

Keywords

information security ontology, human behavioral implications, password policy

1. INTRODUCTION

Increasingly organizations are looking to external, industry-recognized best-practice standards for advice on how best to manage their information security infrastructures (e.g. the ISO27K series, including [1, 2]). By seeking compliance (and in some cases certification) with standards, an organization can not only demonstrate that their information is that much more secure, but also illustrate to customers and business partners alike that they can be trusted to protect important information.

One shortcoming of applying information security standards in a "one-size-fits-all" manner is that there is no outward consideration of the security priorities and working culture of individual organizations [25]. Organizations may differ in many ways, such as in their propensity (and arguably the necessity) to exchange data to leverage business opportunities, and the behavior they wish to encourage within employees regarding the data that they have at their disposal [16].

Information security managers need to understand the usability requirements of the staff within the organization who must live with the consequences of their security decisions [3]. Currently however there is a limited sense of how these users perceive information security within the workplace, and how they choose to react to it [9].

Previous work examining the use of removable USB data-storage devices within organizations [5, 9, 13] has shown that there is a need to consider human-behavioral factors when managing information security policies and security mechanisms. Here we seek to provide a standardized information model for representing these behavioral factors, and how they relate to the security needs of the organization.

We achieve this goal by augmenting the use of best practice information security standards with a structured definition of the associated *human-behavioral implications*, encapsulated within an ontology (i.e. an information model). This informs the decision-making process, allowing managers to account for the identifiable effects (be they direct or indirect) that information security mechanisms have upon individuals within the organization.

As an example, a highly-secure password authentication policy may mandate that users use complex passwords, as a means to reduce the chance of their passwords being guessed or cracked, and thereby provide security. However, mandated password complexity may push some employees (struggling to remember their passwords) to write them down in an unsecured manner. This could conceivably result in a less secure environment than would have been experienced had simpler (and more easily memorized) passwords been employed.

*Corresponding Author.

We frame our work within the context of information security standards compliance, with specific reference to the ISO27002 guideline recommendations [2]. We have selected specific guidelines, and identified potential policy decisions that may be made during the course of their deployment. We focus on those decisions that may impact upon both the security of identified assets and the behavior of employees as they use, or try to use, those assets in accordance with the related security policy. This information is then structured within the provided ontology.

Throughout this work we have consulted an industrial partner representative (a senior information security manager within a large, international financial organization), who is responsible for the computer-system accounts of 50000 staff and 20000 contractors. The organization has successfully applied ISO27K standards, and so our consultations have provided an insight into how our work might be used in practice.

Section 2 discusses the background to our work, primarily the need to consider human behavior as a component of information security, and how use of an ontology can help in doing so. Details of related work in information security ontologies can also be found here. Section 3 introduces our ontology and an example instance of the ontology relating to password policy management. Section 4 provides an evaluation of the suitability and prospective use of the ontology, followed by concluding remarks in Section 5.

2. BACKGROUND

2.1 Information Security & Human Behavior

Information security managers have traditionally focused upon technical controls (e.g. firewalls, e-mail filtering) as a means to secure the information that an organization values. However security managers can ill afford to ignore the human element within the organization [4, 16], which must be put into perspective alongside the security and productivity needs of the organization [10].

Organizations often aim to employ individuals who have a willingness to take risks and exploit opportunities within the workplace to benefit the organization itself. At the same time, this behavior can be regarded as a *human vulnerability*, as it can also create security incidents. Ill-informed or inappropriate attitudes to information security can cause a great amount of damage, be it through careless talk, excessive or accidental distribution of documents, or simply failing to adhere to security procedures [20]. Employee behavior can as such be knowingly insecure, intentionally malicious, or a source of accidental security breaches [15]. That damage can also be expressed in human and social terms, be it a loss of reputation or a soured perception of the organization in the eyes of potential customers or investors.

It is also necessary to develop a sense of the context within which a particular pattern of behavior emerges. Behavior that is beneficial to the organization in one sense (e.g., answering queries from a colleague so as to help them in their work) might constitute undesirable behavior in another (e.g., unknowingly answering queries that are part of a social engineering attack meant to gather authentication details) [4]. This for instance could be resolved by targeted employee education workshops, but managers need to know what behavior it is they are targeting in the first place.

When managing the human element in an information security context, it is necessary to consider both the impact that security mechanisms will have upon the workforce and how people will choose to react to those controls. An individual can ultimately make a decision whether to comply with security policies, and they will be less willing to comply if they perceive those policies as having a detrimental effect upon their primary work tasks [10]. To justify the cost of security controls, it is necessary to establish how effective they are likely to be in practice [4].

The burden put upon an individual by a security control can be measured in different ways, such as a restriction of work capabilities, delayed tasks, or additional processes and information to remember and recognize. This burden can in turn have differing effects upon an individual's attitude towards security, for instance instilling a sense of frustration or futility [19]. Inadvertently influencing a person's attitude in a negative way such as this only fuels the conscious choice to circumvent security controls, or at the least hold them in contempt [16].

A person's attitude towards organizational security can also influence their perception of how they are regarded by their employers [4]. An individual is less likely to seek out new business opportunities for an employer that they feel does all it can to limit their ability to seek out these opportunities. If not properly managed, security controls could become the tool that seemingly works against the goals of the organization.

2.2 Taking Control

Organizations must cultivate an awareness of the human-behavioral implications of their internal information security decisions. The person best positioned to do so would be the internal information security manager (CISO, CIO, etc.) and, if applicable, any members of their team that are normally included in the decision-making process. We refer simply to the 'CISO' as a collective term for such an individual.

Ideally those involved in the decision-making process would have an awareness of the business goals of the organization (and with this associated legal and financial concerns [24]). The propensity for risk, as communicated by senior management, must be adequately represented in the information security policies that are deployed across the organization. Individual employees can (and arguably should) be capable of behaving in a 'risky' manner to further the goals of the organization. CISOs are in a position to ensure that the right risks are free to be taken at the right time, and that risks that senior management do not want to see being taken are prevented all of the time. This provides a challenge to clearly represent and communicate the directives of senior management.

Predicting the usability needs of employees and tailoring the information security infrastructure around them should be a priority [25]. This is especially pertinent as an understanding of information security from a human-behavioral perspective could in turn be used to promote positive security behaviors, thereby pacifying negative perceptions of information security within the organization [4]. Such an understanding could help in identifying, managing, and potentially stemming the causes of persistent problems (e.g. staff forgetting passwords), as opposed to perpetually reacting to the symptoms [16].

2.3 How an Ontology Can Help

Organizations are nowadays driven to frame their security management processes within the context of external security standards. Hence seeing human-behavioral factors through the lens of internal information security controls is not enough. External standards must be tailored to respect the organizational culture, business priorities and usability requirements of the employee base [25]. By aligning information security guidance with the qualities of the organization, standards compliance becomes more viable [30]. We assume here that a CISO can pursue standards compliance without jeopardizing their ability to accommodate the usability requirements of staff with the same sense of priority.

A fully-informed view of information security within an organization must then to some degree include internal controls, external standards, and usability concerns. Provision of a structured information model would go some way towards achieving a holistic view of information security management such as this, in terms of its realization, intent, and its impact upon members of the organization. For example, if a standard recommends deployment of a password authentication system to protect valuable data, a model can be used to relate its properties to the CISO's password policy decisions and the projected end-user experience.

Representing such a view in an ontology would be appropriate for a number of reasons:

- By providing a taxonomy of information security terminology, there is scope for security engineers to broaden their knowledge of related concepts [34], in this case the human-behavioral implications of their security decisions.
- By encapsulating a standardized taxonomy of concepts and terms, an ontology can provide a common language [35], with the potential for improved communication of information security needs and decisions [34]. Differing "auras of understanding", as may be seen between senior management and CISOs, can then be clearly identified and bridged.
- Ontology content can be re-appropriated for other uses, and developed over time [35].
- Use of an ontology provides opportunities for interoperability, not least between different assessment methodologies or software tools [36]. This has the potential to 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.

To be effective it is necessary to relate the human-behavioral implications of information security to the content of external standards. We should also develop some sense of how research pertaining to the human-behavioral implications of information security can be aligned with the requirements of a CISO. This requires a means of representing the complex interrelationships between the different concepts of human behavior and information security.

For this purpose the work undergone here provides an ontology that can be used to demonstrate the potential human-behavioral implications of information security decisions within the context of identified external standards. With this, we approach the challenge of determining how and what information should be represented. Human behavior is arguably too rich and varied to be reduced to an ontology, however we aim to provide the foundation necessary to relate human-behavioral usability factors to technical and procedural security controls.

With our work, the information security decision-making process can be afforded recognition of those instances where the capabilities of security mechanisms reach their limit, and where security can only be strengthened by influencing the human-behavioral factors at play.

2.4 Related Work in Information Security Ontologies & Taxonomies

A number of ontologies have already been developed for purposes relating to information security. It is useful to review these works to better understand what is required of an ontology that relates information security, human-behavior and business concerns.

Work by G.B. Magklaras & S.M. Furnell [41] provides a tool for estimating the level of threat originating from an organization insider, through the configuration and evaluation of user behavior profiles. The argument here is that "all actions that constitute IT misuse lead back to human factors", and furthermore that individuals within an organization have greater access capabilities than those outside. A taxonomy was developed to represent properties of users. This taxonomy includes different behavioral motivations, i.e. intentional and unintentional behavior (e.g. "deliberate ignorance of rules", "inadequate system knowledge"). There are also basic representations of the (traceable) technical-level consequences of insider threats, as well as role definitions based upon user capabilities (e.g. "advanced user"). It is proposed that this taxonomy be used to profile individual users within an organization, and that these profiles be correlated with related system activity to determine the extent of the threat posed by each system user (e.g. "potential threat", "harmless"). This work supports the point that a particular pattern of behavior can have a number of causes, and that a CISO needs to consider the possible outcomes of introducing users and technologies. It also reminds us that we can only manage user behavior that is detectable, and that in our case we need at the least to consider how user behaviors are communicated to the CISO (either directly or through cross-departmental consultation, for instance).

Another investigation into the misuse of information is described in the work of Braz et al [32]. This work is interesting to us as it discusses using high-level policies to mitigate procedural threats. For instance, "verify source of information" would be used to manage a threat of "customer provides false info". The work goes on to describe how policies can be combined, and appropriately implemented as technical security controls. It is often difficult to manage the behavior of individuals with a single security mechanism without stifling the same elements that make them useful to an organization. This work demonstrates the concept of composing controls to influence the potential behaviors within a particular process. Furthermore it also provides examples of information security directives that do not necessarily prohibit activities, but can instead be used to ensure their correctness according to organizational policy.

The ROPE methodology [39] and related security ontol-

ogy [14] provide organization-wide evaluation of IT security management, with a focus on business processes and risk-management. The ontology encapsulates well-known information security concepts such as assets, vulnerabilities, threats and controls. These inter-related concepts are used as a framework for structuring organization-specific knowledge, which is used both for high-level decision-making and as input to the ROPE risk assessment process. The work in [39] and [14] illustrates use of organized infrastructure knowledge as a tool in a holistic security management decision-making process. Our work aims to provide a similarly 'global view' of organizational priorities, aligning security and business objectives. The security ontology in [14] also stresses the need of IT managers to represent and communicate qualities of the IT infrastructure to senior management, as a means to better justify their security decisions and reduce the reliance on intuition. We also aim to utilize an ontology to structure and communicate information security decisions, although at this stage we assume less that intuition will be used, but more that our work can augment and unify disparate assessment methodologies (e.g. as relate to risk assessment or projections of infrastructure investment).

A security ontology incorporating external standards is described in the work of Fenz et al [33]. Here individual guidelines from the ISO27001/2 standards are related to tangible security control implementations within an organization. This provides a means of structuring and assessing internal security policies within the framework of ISO standards. This facilitates a process that requires less effort to align external information security standards with internal policies. These qualities are intended to enable smaller organizations to approach standards compliance, by systematizing more of the compliance process.

The ontology created in [33] acts as the foundation for a software application provided to manage the assessment of security control effectiveness. The work is built upon in [6] to provide a methodology and tools for stipulating control-selection criteria while pursuing ISO27001 compliance. We envisage that our work could also be augmented with relevant assessment tools, albeit not as tightly as is demonstrated here.

Work by Seok-Won Lee et al [38] describes the derivation of security requirements from external standards (including US Department of Defense guidelines). The work provides a process for determining interdependencies across content from different standards, and the development of questionnaires for use in adapting standards to internal security configurations. This work demonstrates adaptation of natural-language security standards to internal security infrastructures, including the identification and association of assets, threats, vulnerabilities and controls to guideline content requirements, by way of information models. This approach is used to help predict and understand how standards will function in practice, by relating them to an organization's technical infrastructure. In our work we use an ontology to relate standard content to the perception and compliance of individuals towards security within an organization, by way of the effects that the security infrastructure has upon internal working practices.

OntoSec [36] is a security ontology for use in structuring security alerts within the security function of an organization. This work aims to provide a standardized taxonomy for security events originating from disparate security mechanisms, and represent the relationships between these events. Usage data from security mechanisms is translated into ontology content, and tools are provided to facilitate querying of this data to identify patterns of network security events. A security manager would then use this information to efficiently develop controls based upon the recorded qualities of previous computer security incidents. In our work we also develop an ontology as a means to structure knowledge about past events for use by a security manager (in our case a CISO). However instead of sample data relating to security controls, we intend to populate our ontology with observations and structured reasoning as derived from informed research into the usability of information security policy mandates.

2.5 Requirements

The previous discussions regarding information security ontologies and human behavior have highlighted a number of requirements that we must consider when developing an ontology:

- The behavior of staff should adequately represent the organization's business and risk management strategies. The usability and security behaviors of staff must then be considered as part of an organization's information security policies. This includes identification of:
  - the vulnerabilities that IT users create;
  - the intentional or unintentional threats user actions pose to organizational assets and the information security infrastructure, and;
  - the potential process controls that may be employed to manage user behavior, and their identifiable effects upon that behavior.
- Information security mechanisms are guided by policies. These policies are increasingly informed by external standards. This should be recognized and accommodated in the ontology.
- CISOs must be able to relate the content of the ontology to the information security infrastructure they manage, and the decisions they make regarding this infrastructure. Ontology elements representing human factors and external standards should then be combined in a manner that will prove useful in the information security decision-making process.

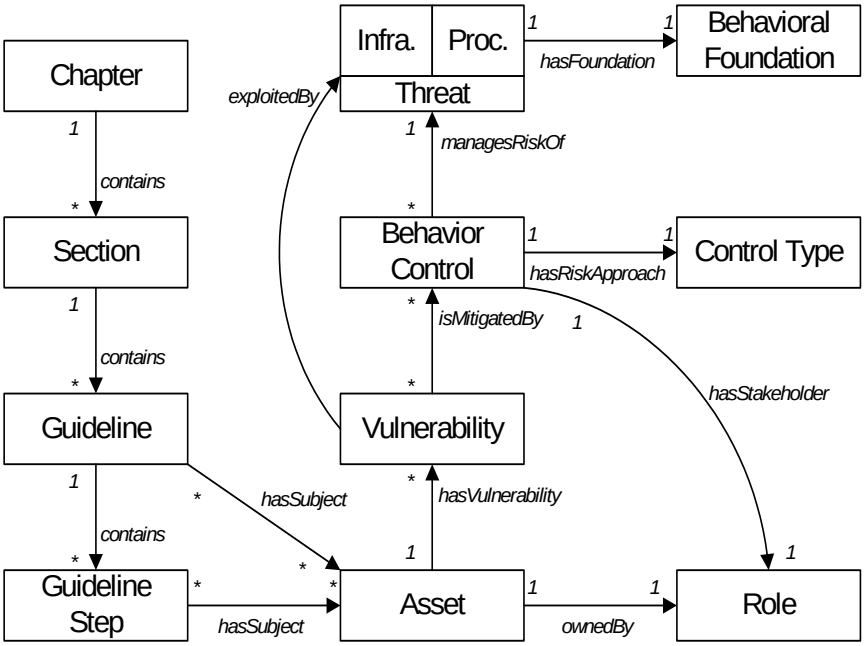

Figure 1: Overview of the information security ontology.

3. DESIGN

Here we introduce an ontology that represents attributes of external information security standards, and aligns these with the potential *human-behavioral implications* of their implementation. This requires us to divide the content of a standard into its constituent components, reaching a level where individual security processes and controls can be associated with the usability concerns that they may illicit in practice. In this sense we essentially overlay a human factors ontology onto an information security ontology.

Within the ontology we represent the security weaknesses of an organization's assets. These weaknesses may promote or inhibit certain employee behaviors. These behavior patterns are then modeled as potential threats. These may be threats to security (e.g., an employee persistently forgetting a password and choosing to have it written down in clear view) or threats to productivity (e.g., an employee forgetting a password, then requesting the password be reset, thereby being unable to continue their primary task in the interim). We further represent the procedural control decisions that a CISO can enact to manage those threats.

We regard external standards as the framework for our ontology. We assume that information security managers should have the capacity to intentionally or otherwise stray beyond the static definition of compliance if they believe it to be beneficial to the organization. The context then becomes the achievement of a balance between security, user policy compliance and budget/board constraints. An instance of the ontology can provide record of the approaches taken towards specific security (and arguably business) risks, which the CISO then uses as evidence for making judgments.

Our work uses the ISO/IEC 27002 standard [2] as a framework within which to develop the content for our ontology. The recommendations of the ISO27002 standard are intended to be built upon an Information Security Management System (ISMS) as described in the accompanying ISO27001 standard [1]. We make a similar distinction to the one made in [33], separating the controls detailed in the standard into 'hard', physical security aspects and 'soft', organizational security aspects. At this point we do not consider 'softer' controls (e.g. those concerned with user education & training).

We do not consider technical- or configuration-level concerns in our ontology (e.g. the mandated length of passwords or the required character sets). New or alternative technologies tend to emerge with greater regularity than security standards, and so we focus on high-level, procedural controls. Other works make a similar distinction, so as to focus on the development of high-level process controls that then guide technical-level solutions (e.g., [22, 32, 35]).

During development of our ontology, we followed the advice for creation of ontologies outlined in [40]. Adhering to the associated recommendations guaranteed that the structure of our ontology would be consistent, robust and usable.

Our ontology has been implemented in the Ontology Web Language (OWL) [17]. We use OWL as it is a well-supported ontology language, and there are code libraries available to facilitate building software applications on top of the ontology in the future should we choose to do so. We used the Protégé Ontology Editor application [18] to construct the ontology and enter data for our applied example (as further detailed in Section 3.7).

3.1 Overview

As shown in Figure 1, our ontology is comprised of a number of different concepts. Each individual concept has a relationship with one or more other concepts. The objects `Chapter`, `Section`, `Guideline` and `Guideline Step` provide representation of content from the ISO27002 information security standard. An individual `Guideline` can be associated with a particular `Asset` by way of the '`hasSubject`' relation. Otherwise if a `Guideline` is broken down into more

refined Guideline Steps it will be these that are linked to Assets. We represent those Assets identified in a Guideline or Guideline Step that either must be secured or which are crucial to a security process. In our ontology an Asset can be 'ownedBy' someone that has an identified Role.

It is with the Vulnerability object class that we introduce human-behavioral factors into the ontology. The security or usability of an Asset could be put at risk by an identifiable form of human behavior (e.g., "memorization of password difficult").

A Vulnerability may be 'exploitedBy' a Threat (e.g., "password forgotten"), which renders the Asset unusable or insecure. A Threat may be either an Infrastructure Threat or a Procedural Threat. The former represent activities within the security infrastructure that impact upon the usability of security mechanisms, whereas the latter represent events within a security-oriented process where humans interact with security mechanisms. With each Procedural Threat we record the Behavioral Foundation of the threat, as a means of classifying behaviors and indicating the concerns that they raise within the organization (e.g., someone's memory capabilities or attitude towards security in the workplace).

A Vulnerability may be 'mitigatedBy' a Behavior Control. A Behavior Control represents a procedural activity that can be enacted to manage the interactions between humans and organizational security controls. Each Behavior Control has a Control Type which indicates the risk management approach it takes, so that a Behavior Control 'managesRiskOf' a specific Threat.

Further details regarding each of these concepts and their interrelationships are described in the following sections.

3.2 Chapter, Section, Guideline & Guideline Step

In the case of the ISO27002 external standard, content is broken into Chapters. Each Chapter refers to a general area of information security management (e.g. "Access Control", "User Training & Education"). Each Chapter has a number of Sections, which each address specific areas of the Chapter's subject matter. Each Section describes a number of Guidelines, detailing specific procedural concerns (e.g. "User Password Configuration", "Notifying New Employees of Terms of Use"). For each Guideline in the ISO27002 document there are a series of 'Implementation Guidance' Steps (referred to here as Guideline Steps), describing prescribed methods for achieving compliance with the named guideline. An individual Guideline Step then describes some best-practice advice on how to safeguard a named asset within the wider process.

We resolve the discourse between external standards and infrastructure concepts (such as threats and controls) by associating infrastructure concerns with specific Guidelines or, where a Guideline has been refined further, individual Guideline Steps. We accept that the standards structure we have chosen is tightly-bound to the structure of the ISO27002 document. However, it is not inconceivable for other external standards to be modeled also (owing to the natural extensibility provided with use of an ontology).

3.3 Asset

Within the ontology an Asset is an identifiable artifact which is of value to the organization (be it monetary or as a means to further the organization's business goals). This could be something tangible such as a computer or printer, or something intangible such as sensitive business knowledge. By identifying the assets which are of importance to the organization, and the security processes that can be employed to secure those assets (as detailed in the ISO27002 standard), it is possible to begin informing the development of internal policies for their protection.

The ontology must reflect or represent the asset manifest of the organization. It is then appropriate to record the 'owner' of the Asset, which may be selected from an organization-specific set of role definitions.

3.4 Vulnerability

An Asset may exhibit some weakness that makes it susceptible to exploitation (either directly or indirectly). Such a weakness is referred to as a Vulnerability. We choose to concentrate our efforts on identifying those vulnerabilities exposed in security processes that may be exploited directly or indirectly by human behavior, whether that behavior is intentionally malicious or unintentional (such as mistakes or oversights). An example of such a Vulnerability would be burdening a user with an additional password to remember, which on top of having to already remember any number of work-related passwords may cause that individual to forget or confuse one or more old and new passwords.

At this stage we rely on the judgment of the CISO to determine whether a given Vulnerability is exhibited by their information security infrastructure. Since each Vulnerability we identify is based in a potential pattern of behavior, and less in a technical configuration, this essentially requires a judgment on the capabilities and working culture of the workforce.

With this we consider both *behavior that affects security* and *security that affects behavior*, as one can influence the other. A Threat (described in Section 3.5) to a Vulnerability essentially constitutes the former, and a Behavior Control (see Section 3.6) the latter. As an example, if in a given organization a culture of complete trust was in effect, a password-authentication system might not be deployed, but deploying such a system might make individuals question who and what they trust.

3.5 Threat

An Asset may be perceived as vulnerable to some form of exploitation, but that is not to say that it will necessarily be exploited. A Vulnerability becomes a problem when there is some means of exploiting it (a Threat) and a probability of that Threat manifesting.

In our ontology we make a distinction between those threats that affect the infrastructure of an organization (e.g. "IT help desk too busy to answer password-reset requests"), and threats that affect the human-oriented procedures and usability requirements inherent in using a particular Asset (e.g. "user has forgotten system log-on password"). We refer to the former as Infrastructure Threats, and the latter as Procedural Threats.

Note that the Threats that we consider may not directly affect the security of an organization's Assets. However, they may otherwise have an effect upon productivity, and so should any such Threats manifest, they may adversely affect an individual's attitude to security. If security measures are not attuned to an individual's usability requirements, they

Table 1: Types of Behavioral Foundation

Cultural	Different cultural practices may exist across geographic (or perhaps even social) boundaries
Ethical	Basic ethical considerations should be noted, e.g. personal privacy
Temporal	Conditional changes may exist based upon the time of day or the duration of an event (e.g. employees may lose focus on their work or have diminished patience at the end of the working day)
Mindset	Someone's disposition could indicate that they may behave maliciously or opportunistically with respect to the organization's assets
Capability	There may be individuals within the workforce who have some form of physical impairment. This may affect their ability to interact with security mechanisms

Table 2: Refined 'Mindset' types

NAME	ASSOCIATION	INTENT	DESCRIPTION
Friend	Internal	Non-Malicious	A Friend may behave in an unintentionally non-secure way, or may otherwise be unaware of the value of security in relation to their primary task
Outsider	External	Non-Malicious	A party outside of the organization who, like a Friend, can be assumed to never have any malicious intentions. However, just like a Friend an Outsider may exploit a vulnerability unintentionally
Traitor	Internal	Malicious	Assumed to have malicious, targeted intentions. A Traitor seeks out specific assets within the organization, and the means to exploit those assets
Foe	External	Malicious	A malicious party operating outside of the organization. A Foe can be assumed to have intentions to obtain or exploit specific assets. A Foe could be an individual hired by the organization, e.g. hardware/software support staff, or even a business partner
Opportunist	Internal	Opportunistic	May be someone inside the organization who has malicious intentions with no particular target. An Opportunist will exploit any vulnerability, for personal gain or satisfaction (e.g. amusement)
Outside Opportunist	External	Opportunistic	The external equivalent of an Opportunist

may feel inclined to sidestep security measures that they regard as cumbersome in order to "get the job done". As such, we identify potential `Threat`s to the *desirable security behavior* of an organization.

We record the potential consequences of each `Threat` should it occur (as also provided by e.g., [36, 37]). We do so informally, although effort is made to represent the consequences in terms of the potential impact of a `Threat` upon individuals within the organization.

Regarding the probability of a Threat manifesting, we assume that a CISO would use their own experience to determine the likelihood of a `Threat` occurring, or more likely some methodologies external to the ontology. There is also no sense of the passage of time within the ontology, and as such no measure of how compounded security behaviors may affect an individual (i.e. how human-behavioral implications may influence each other when aggregated from multiple `Threat`s over time).

3.5.1 Procedural Threat

`Procedural Threat`s are essentially events that constitute a conflict of usability and security instigated by an individual within the organization. It is beneficial to have a basic understanding of the aspect of individual or societal behavior that drives the `Procedural Threat`. We refer to this as its `Behavioral Foundation`. The `Behavioral Foundation` then allows us to classify a `Procedural Threat`, and examine it in the context of the desirable security behavior of the organization. Table 1 shows a table of the basic types of `Behavioral Foundation` that we have considered in our work.

The `Behavioral Foundation` also informs the level of sensitivity required when addressing a `Procedural Threat`. An individual who tells a 'trusted' colleague their password in confidence in case they believe they might forget it themselves should be approached differently to an individual who, without prompting, tells their password to a colleague simply because they do not acknowledge the security value of that password. The solution changes based upon the nature of the `Threat`. Forgetfulness may (or may not) be accommodated by placing reminder signs in prominent places or through security training workshops. Ignorance might be stemmed through the careful use of sanctions (thereby forcing the individual to address the source of their own ignorance).

In the case of a person's security 'Mindset' we have seen fit to define the scope of different actor behaviors, based on those defined in [9]. These relate motives to behavior, as a marker to refine the means of altering or countering that motive. One potential application of refining the scope of a `Behavioral Foundation` would be in establishing which aspects of the information security policy should be targeted within staff education programs (e.g. relating to the disclosure of personal security details to outside callers). The refined behavior types within the scope of the 'Mindset' `Behavioral Foundation` are shown in Table 2. Refined scopes for other kinds of `Behavioral Foundation` can also be defined.

3.6 Behavior Control

There may be a number of methods available for the management of each human-behavioral `Vulnerability`. We approach each individual `Vulnerability` through the potential application of system-wide policy or infrastructure changes. We then refer to these high-level directives as `Behavior Control`s. We would for example consider a mechanism of policy change at a level of "make passwords more complex" over "include one or more punctuation characters in man-

Table 3: Types of Risk Approach

Retention	Explicit acceptance of any risks that arise from the existence of an identified `Threat`
Reduction	Identifies a `Behavior Control` that is deployed in an attempt to reduce the possibility of a `Threat` manifesting
Transfer	Used to record those `Behavior Control`s managed by an external party. It could also apply to a distinct and separate function within the organization (e.g. the transfer of password reset burden onto the internal IT help desk function)
Avoidance	Action may be taken to completely avoid an identified `Threat`

dated password content".

Since each `Behavioral Control` essentially describes a procedural solution, it is up to the judgment of the CISO to decide how to enact the control in reality. Our approach leaves a CISO free to consider different solutions equally, without necessarily favoring one over the other. Our methodology also aligns with the use of external standards, as standards typically prioritize processes over technologies.

Work by Neubauer et al [6] discusses representing "countermeasure side-effects". Our ontology represents the usability-oriented side-effects of deploying a `Behavior Control` by way of its human-behavioral implications. In our ontology it is possible for a `Behavior Control` to have its own associated `Vulnerability` types. For instance, an unwieldy password authentication system could be mitigated by relying on token-based security - it is then conceivable that employees could lose their tokens. In this sense our ontology can inform information security managers of the human-behavioral implications of the `Behavior Control`s they intend to implement.

3.6.1 Control Types

Decisions relating to information security management must be explicitly agreed by senior management if they are to have the resources they need. This is not simply a case of mitigating every `Vulnerability` or neutralizing every `Threat`, as senior management may regard the associated costs or resultant restrictions on user behavior as too great to be justified. The choices that are made must reflect both the organization's stance towards risk propensity and its working culture. These can only be determined through communication with those who run the organization.

To this end we associate a `Control Type` with each `Behavior Control`, as a record of the risk management approach that the control offers towards a particular `Threat`. A table of the basic risk approaches we use is shown in Table 3.

An example of the use of `Control Type`s might be with passwords that are difficult to remember. There is a `Threat` that staff may forget their passwords, which could be targeted by making passwords simpler. However, another `Behavior Control` might be to maintain the same policy, but employ IT help desk staff to deal with password resets. This does not make passwords any easier to remember (thereby side-stepping the `Threat`), but manages the implications of the `Vulnerability`. In this sense a `Behavior Control` can be used to promote a specific vision of ideal security behavior within working practices.

A stakeholder role can be associated with each `Behavior Control` to clarify who should be consulted before enacting a particular process strategy. For instance, choosing to enforce complex passwords is likely to result in a number of passwords being forgotten, and with this a number of password-reset requests being directed to the organization's IT help desk (if they have one). The manager of the help desk would need to be consulted in this event.

3.7 Example - Password Policy

To assess the efficacy of our work we examined specific ISO27002 guidelines and encoded them in the ontology. Here we examine one of those examples.

Researchers have already investigated the usability issues associated with passwords (e.g., [7, 8, 11]). Here we aim to align some of the concepts of this research with the act of maintaining compliance with an external standard (in this case ISO27002). By combining existing information security standards and methodical research regarding usability issues, we bring together industry-proven management guidelines and assessments of structured research observations.

To provide an example of how our ontology might be applied, we examined existing research to identify issues that users typically raise when using passwords (e.g. "forgetting password", "use of recall aids").

We selected a guideline within the ISO27002 standard relating to password policy, specifically `Guideline Step` (b) of `Guideline` 11.3.1, "Password Use". We then identified a user's Password as the `Asset` requiring immediate protection (since it can be implied that gaining a Password gains access to business data). Once the `Asset` had been identified, we conceived a series of human-behavioral `Vulnerability` types, `Threat`s and `Control`s that must be considered.

The ontology then serves to represent the possible permutations of perception relating to passwords, as viewed from the perspectives of both a human user and a CISO within an organization. A sample of the example ontology content is shown in Figure 2. This sample focuses on one root Vulnerability relating to a user's Password.

Within the example we identify a number of concerns linked to password policy, as described in the following discussions. By describing these concerns we illustrate that a CISO must understand the impact that their information security decisions will have upon individuals within the organization, both in the behavior that these decisions elicit, and the behaviors that must be carefully managed to maintain security.

3.7.1 Password Memorization

From the identified `Asset` Password, there is a `Vulnerability` entitled "Single Password Memorization Difficult". This represents the possibility that an individual could have trouble remembering a password of the complexity required by the organization's password policy.

There are a number of behavioral `Threat`s which may exploit this weakness. A Password may be forgotten, perhaps due to an individual's Capability (or more precisely their memory). The consequence of this would be that the individual would be without system access until they could remember their password or have it changed.

The organization may accept that this is a possibility and choose to "Maintain Password Policy" as a `Behavior Control` (choosing perceived security over usability). Otherwise a choice may be made to "Make Password Easier To Remem-

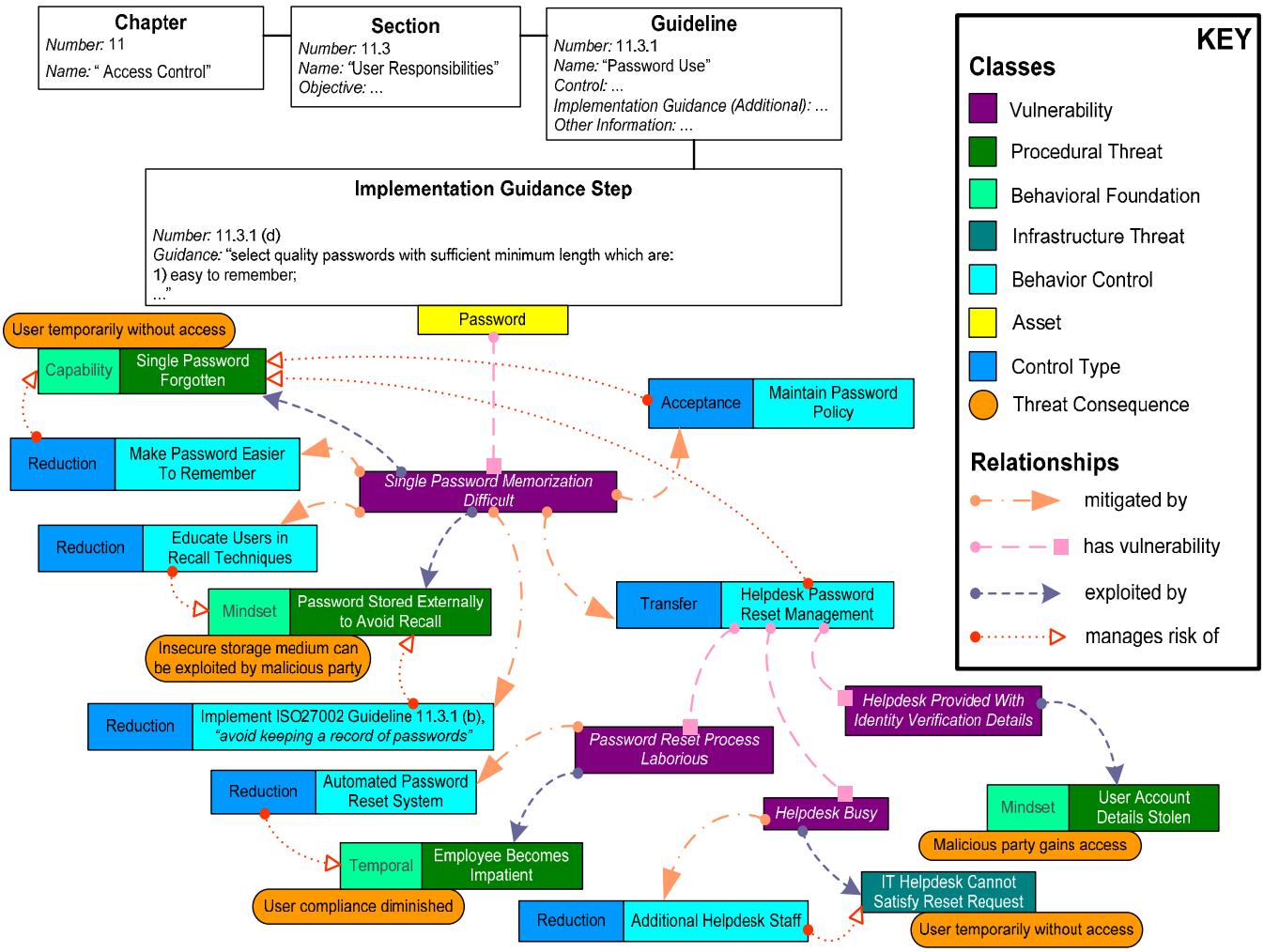

Figure 2: Sample of ontology content relating to password policy.

ber", thereby reducing the chance of someone forgetting their Password (potentially at the cost of perceived security).

3.7.2 Managing Password Recall Methods

If an individual is having difficulty remembering a Password, it is possible that they will for instance write their Password down, or use some other form of external record of the Password to avoid the need to recall it when needed. An insecure record of the Password (e.g., a piece of note paper next to the user's workstation) could then be exploited by a malicious party.

One method of reducing the need for users to record their Password externally would be to "Educate Users in Recall Techniques", helping them learn to remember Passwords with less effort. Another approach to the problem of insecure records of Passwords would be to enforce a 'clear desk' policy, whereby users are not permitted to leave any artifacts at their desks which may contain or allude to secure information. This `Behavior Control` does not solve the problem of users forgetting their passwords, but would reduce the range of insecure behaviors that users exhibit.

3.7.3 Password Reset Function

Organizations can choose to rely on internal IT help desk facilities to balance the security and usability of passwords [8]. This then allows a staff member to make a request to have their Password reset to a known string of characters (which they then may be able to remember, or otherwise may forget again).

If the password policy is fixed, staff could be provided with the option to utilize a "Helpdesk Password Reset Management" `Control` function. This would then transfer the cost of managing forgotten passwords to an internal or external helpdesk team.

If an IT helpdesk team must carry the cost of users forgetting their `Password`s, it is likely that such a cost would be measured in the number of reset requests that the helpdesk must respond to. It is possible that if a great number of system users are having difficulty remembering their passwords that the helpdesk will be too busy to answer requests promptly. This would extend the time for which callers are without access to the system. One obvious solution is to employ "Additional Helpdesk Staff" in an effort to reduce the number of callers left waiting to be answered.

An individual may find the "Password Reset Process Laborious", growing impatient with the time it requires. A consequence of this would be a reduced willingness to comply with the process, especially if it detracts from the calling individual's primary work tasks. One answer to this would be to introduce an "Automated Password Reset System" (assuming here that such a system would require less time than a helpdesk member to issue a new `Password`).

One final `Vulnerability` introduced by use of a helpdesk function is that a member of the helpdesk team must typically be provided with details verifying the identity of a caller (to ensure the distribution of passwords to the correct recipients). However, a malicious party within the helpdesk team may exploit these details to gain access to an individual's system account. There is then the need to consider that employing a helpdesk function to increase usability may also introduce its own security problems.

4. EVALUATION

4.1 Applicability

During development of our ontology and example content we consulted a large IT consultancy, a representative from a large financial organization, and human factors researchers. This provided insight into the requirements and usability needs of prospective users of the ontology.

With reference to the ontology evaluation criteria outlined in [27], consultation with potential users of the ontology has provided us with assessment of its syntax, usability and content requirements. In consulting human factors researchers regarding our password policy example (as described in Section 3.7), we made effective use of expert knowledge to guarantee the completeness, correctness, and consistency of the ontology content that we have developed.

By following guidance on ontology development [40] and encoding our ontology in OWL, we have served to demonstrate that the concepts in our ontology are well-defined and that the relationships between those concepts are precise. The use of OWL also provides us with application-based evaluation of the ontology content [29].

4.2 Envisaged Use of the Ontology

Our ontology has the potential to provide a unique perspective on the human-behavioral factors associated with information security standards compliance.

Ideally organizations would have both an IT security analyst and a human-behavioral expert in their employ. With this we envisage that distinct surveys would be conducted to identify specific information security mechanisms as described in an external standard, along with the associated human-behavioral concerns.

Concerning external standards and their place in our ontology, we would advocate the decomposition of standards into policy directives by way of a top-down approach, as described in [42]. This involves breaking a standard down into individual guidelines, which then form the requirements for the development of internal security policies. It is necessary for CISOs to translate these policies into a workable solution for distribution across the organization [24]. We envisage that our ontology would be used as a precursor to this translation process, providing a perspective on how policy directives might affect employee behavior before those directives are realized.

We envisage that population of the ontology with potential human-behavioral implications and controls will require targeted studies relating to each specific security mechanism to be conducted. We have already demonstrated in our example how research relating to human factors in password authentication mechanisms can be appropriately incorporated into our ontology, by associating structured expert knowledge with relevant guideline recommendations in the ISO27002 standard.

Population of the ontology with human-behavioral properties would rely for the most part on the examination of security behaviors that are readily observable i.e. high-frequency events that have a limited, perhaps predictable impact upon the security infrastructure or the security behavior of the employee base. Although this approach is not immediately able to identify rare, potentially complex and high-impact events [26] it may however be possible for a CISO to use our ontology to better envisage the composition of multiple

human activities, as typically contribute to complex security incidents.

The ISO27K standards that we have examined in this work inform the management of business risk as relates to information security. It is as such logical to include representatives from each area of the organization affected by information security in the compliance process [23]. Our ontology is well-placed to provide natural language recommendations in a structured manner, promoting an inclusive approach to information security management.

An approach of consultation similar to that described in [31] would facilitate effective use of our ontology within a particular organization. Herein a first step is to identify business processes and security properties within the organization e.g., Assets, Threats, Controls etc., as for instance identified in existing resource manifests (a process wherein use of an ontology is recommended). The Threats and Controls would in this case be the behavioral processes that may either manifest or be imposed upon the organization's staff.

Our ontology provides a unifying medium for communicating the usability requirements of different departments and work roles to the security function, as the potential threats to productivity and opportunities to promote security behaviors are made more apparent through its content.

Following from this we would rely on information security managers to use the gathered information to make judgments regarding their management options. This judgment process may be augmented with other forms of risk/benefit calculations. The primary use of our ontology is as a guide to the usability factors that must be addressed when deriving information security policy within an organization, and so we would assume that the ontology would be integrated into a broader framework of external standards and industry best-practice knowledge.

5. CONCLUSION

We have investigated the need to understand the usability requirements and attitudes towards security that exist within an organization, so as to ensure that information security management is effective. We have built upon this with an information security ontology that combines the content of external information security standards with explicit representation of potential human-oriented security concerns. This ontology provides a framework within which to investigate the human-behavioral implications of information security management decisions before security controls are deployed.

We conclude that it is possible for organizations to consolidate information security policies with human-behavioral considerations, and that this process can be facilitated through use of a specialized ontology. Our ontology has demonstrated that expert knowledge of usability factors in information security can be associated with information security infrastructure properties. We have shown that our method of associating security infrastructure properties with their human-behavioral implications can identify potential user behaviors or effects upon this behavior before they are realized within the organization. This knowledge can be used to promote more usable security infrastructures.

Alongside this work we have been actively investigating the usability issues of the ontology from the perspective of an information security manager. For this purpose we have been progressively integrating the ontology into a prototype 'Knowledge Base' application [28].

6. 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 to Robert Coles (Merrill Lynch), and Adam Beautement (University College London) for their contributions to this work.

We would like also to thank our industrial and academic partners on the Trust Economics project [12] for their continued feedback and support.

We are also grateful for the insights and comments offered by Howard Smith (Sunderland City Council, UK), Maciej Machulak and Dasha Stepanova.

7. REFERENCES

[1] British Standards Institution, "BS ISO/IEC 27001:2005 - Information Technology – Security Techniques – Information Security Management Systems – Requirements", 2005

[2] British Standards Institution, "BS ISO/IEC 27002:2005 - Information Technology - Security Techniques - Code of Practice for Information Security Management", 2005

[3] R. Briggs & C. Edwards, "Skills for Corporate Security", The Business of Resilience, Demos, 2006

[4] KTN Human Factors Working Group, "Human Vulnerabilities in Security Systems: White Paper", Cyber Security Knowledge Transfer Network (KTN), 2007

[5] S.E. Parkin, R. Yassin Kassab, A. van Moorsel, "The Impact of Unavailability on the Effectiveness of Enterprise Information Security Technologies", In Service Availability. 5th International Service Availability Symposium (ISAS 2008), Springer, pp 43-58, 2008

[6] T. Neubauer, A. Ekelhart, S. Fenz, "Interactive Selection of ISO 27001 Controls under Multiple Objectives", Proceedings of the 23rd International Security Conference (SEC 2008), Springer-Verlag GmbH, p. 477-492, 2008

[7] R. Shay, A. Bhargav-Spantzel, E. Bertino, "Password Policy Simulation and Analysis", Proceedings of the 2007 ACM Workshop On Digital Identity Management (DIM '07), pp 1-10, 2007

[8] S. Brostoff & M.A. Sasse, ""Ten Strikes and You're Out": Increasing the Number of Login Attempts can Improve Password Usability", in CHI 2003 Workshop on Human-Computer Interaction and Security Systems, 2003

[9] 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

[10] 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

[11] A. Adams, M. A. Sasse, P. Lunt, "Making Passwords Secure and Usable", Proceedings of HCI on People and Computers XII, pp 1-19, 1997

[12] Newcastle University UK, "Trust Economics Website", `http://www.trust-economics.org/`, last viewed 24/02/09

[13] 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

[14] 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

[15] Cyber Security Knowledge Transfer Network (KTN) & Economic & Social Research Council (ESRC), "The Economics of Information Security", ESRC Seminar Series, 2008

[16] ISACA, "An Introduction to the Business Model for Information Security", ISACA, 2009

[17] W3C, "OWL Web Ontology Language Overview", http://www.w3.org/TR/owl-features/, 2004, last viewed 24/02/09

[18] Stanford Center for Biomedical Informatics Research, "The Protégé Ontology Editor and Knowledge Acquisition System", http://protege.stanford.edu/, last viewed 24/02/09

[19] P. Dourish, R. Grinter, J. Delgado de la Flor, and M. Joseph, "Security in the Wild: User Strategies for Managing Security as an Everyday", Practical Problem. Personal and Ubiquitous Computing, 8(6), pp 391-401, 2004

[20] Information Security Awareness Forum (ISAF) & Information Assurance Advisory Council (IAAC), "Creating a Strong Information Handling Culture", http://www.iaac.org.uk/Portals/0/23176_DIAN_A5_PEOPLE_15_4.pdf, last viewed 24/02/09

[21] A.S. Patrick, "Human Factors of Security Systems". Invited presentation to the HTCIA Atlantic IT Security Professional Development Day, Sept. 30, Fredericton, N.B., 2008

[22] H. Mouratidis, P. Giorgini, G. A. Manson, "An Ontology for Modelling Security: The Tropos Approach", 7th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES), pp 1387-1394, 2003

[23] B. Karabacak & I. Sogukpinar, "A Quantitative Method for ISO 17799 Gap Analysis", Computers & Security, 25(6), pp 413-419, 2006

[24] N. Nagaratnam, A. J. Nadalin, M. Hondo, M. McIntosh, P. Austel, "Business-Driven Application Security: From Modeling to Managing Secure Applications", IBM Systems Journal, 44(4), pp 847-868, 2005

[25] P. Skidmore, "Beyond Measure", Demos, 2003

[26] R. Briggs, "Joining Forces", Demos, 2005

[27] A. Gómez-Pérez, "Towards a Framework to Verify Knowledge Sharing Technology", Expert Systems with Applications, Vol. 11, No. 4, pp 519-529, 1996

[28] D. Stepanova, S. Parkin, A. van Moorsel, "A Knowledge Base for Justified Information Security Decision-Making", CS-TR-1137, Technical Report Series, School of Computing Science, Newcastle University, UK, 2009

[29] J. Brank, M. Grobelnik, D. Mladenic, "A Survey of Ontology Evaluation Techniques", In Proceedings of the Conference on Data Mining and Data Warehouses (SiKDD 2005), 2005

[30] R. Gururajan & V. Gururajan, "An Examination into the Role of Knowledge Management and Computer Security in Organizations", The 7th International Research Conference on Quality, Innovation & Knowledge Management, 2005

[31] T. Neubauer & J. Heurix, "Objective Types for the Valuation of Secure Business Processes", Proceedings of the Seventh IEEE/ACIS International Conference on Computer and Information Science (ICIS 2008), pp 231-236, 2008

[32] F. A. Braz, E. B. Fernandez, M. VanHilst, "Eliciting Security Requirements through Misuse Activities", Proceedings of the 2008 19th International Conference on Database and Expert Systems Application (DEXA), Pages 328-333, 2008

[33] 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

[34] D. G. Firesmith, "A Taxonomy of Security-Related Requirements", International Workshop on High Assurance Systems (RHAS'05), 2005

[35] A. Vorobiev & N. Bekmamedova, "An Ontological Approach Applied to Information Security and Trust", ACIS 2007 Proceedings, 2007

[36] L. A. F. Martimiano & E. S. Moreira, "The Evaluation Process of a Computer Security Incident Ontology", 2nd Workshop on Ontologies and their Applications (WONTO'2006), 2006

[37] J. Undercoffer, J. Pinkston, A. Joshi, T. Finin, "A Target-Centric Ontology for Intrusion Detection", In Proceedings of the IJCAI-03 Workshop on Ontologies and Distributed Systems, 2004

[38] 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

[39] 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

[40] 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

[41] G. Magklaras & S. Furnell, "Insider Threat Prediction Tool: Evaluating the probability of IT misuse", Computers & Security, vol. 21, no. 1, pp 62-73, 2002

[42] F. N. do Amaral, C. Bazilio, G. M. Hamazaki da Silva, A. Rademaker, E. H. Haeusler, "An Ontology-Based Approach to the Formalization of Information Security Policies", Proceedings of the 10th IEEE on International Enterprise Distributed Object Computing Conference Workshops (EDOCW), pp 1, 2006